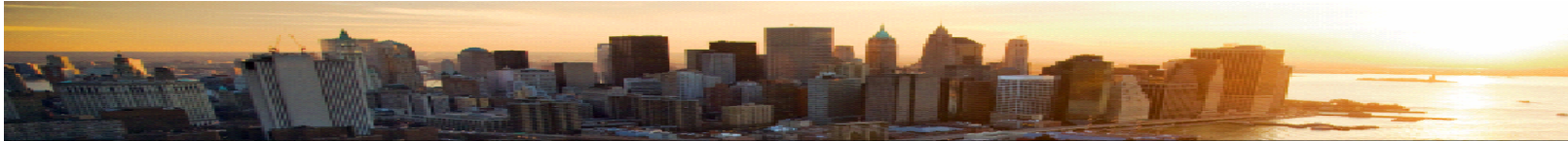




IBM Security Forum
Soluções para um ambiente seguro

Proteção de alto-desempenho para *Backbones*

Nelson Brito
Senior Security Engineer
nbrito@br.ibm.com

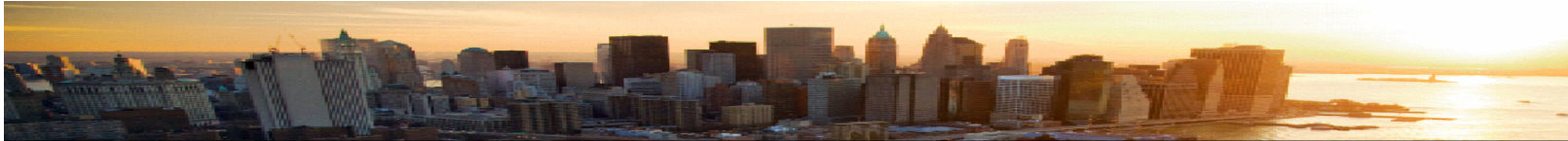


Agenda

- Redes 10 Gbps
- Padrões de Redes 10 Gbps
- Ameaças no *Backbone*
- Exemplos do mundo real
- *Intrusion Prevention System*
- IBM Proventia® Network Security Controller
- IBM Proventia® Network IPS for Crossbeam®
- Perguntas e Respostas



IBM Security Forum
Soluções para um ambiente seguro

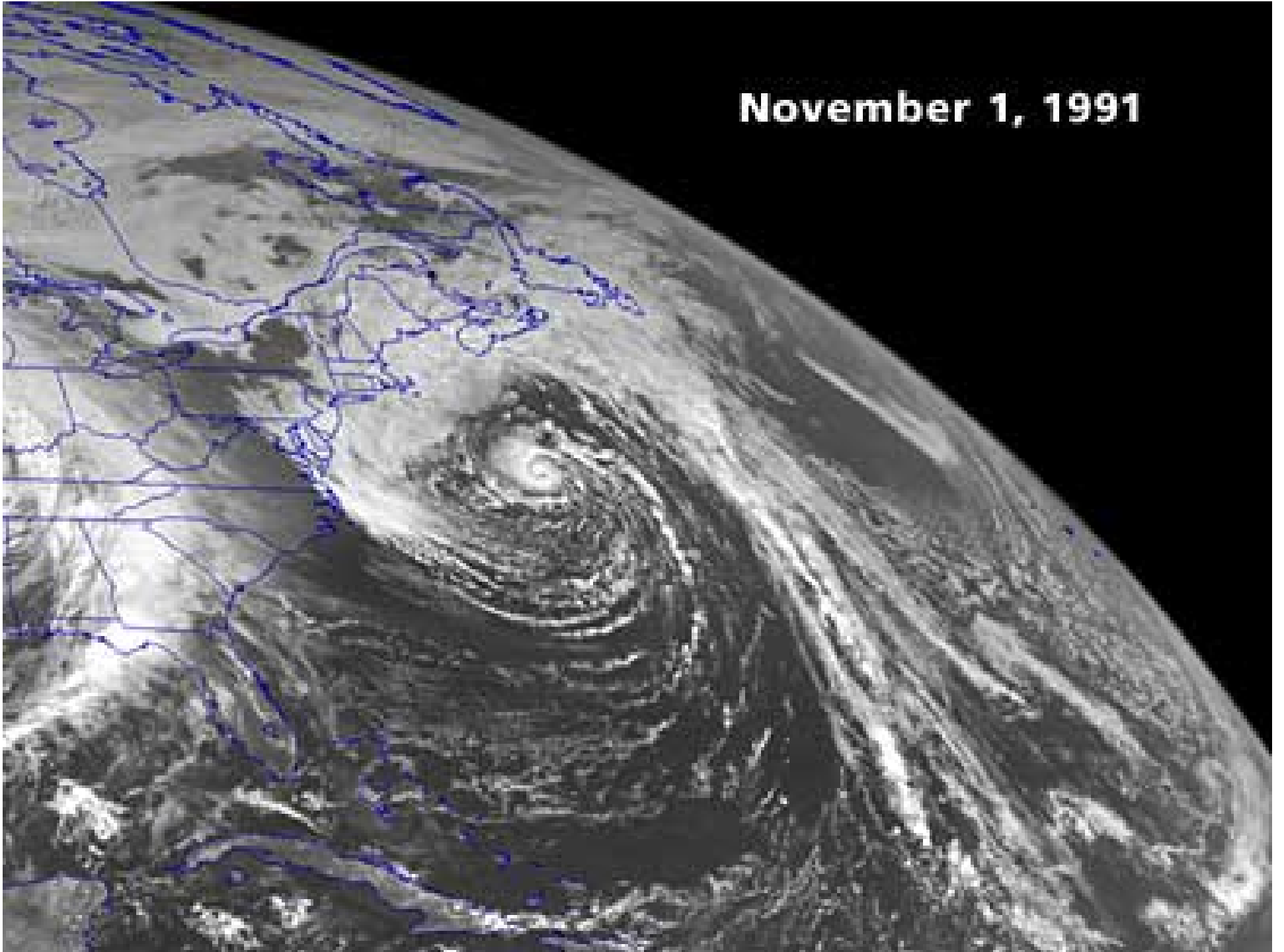


VOCÊ ESTÁ PREPARADO PARA ENFRENTAR A TEMPESTADE DAS REDES DE ALTO-DESEMPENHO?

IBM Security Forum
Soluções para um ambiente seguro

© 2009 IBM Corporation

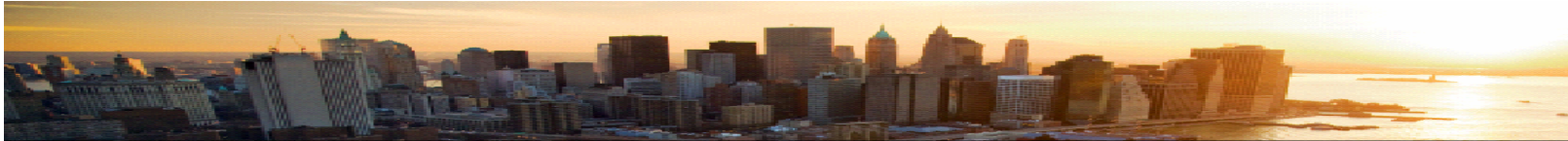
November 1, 1991



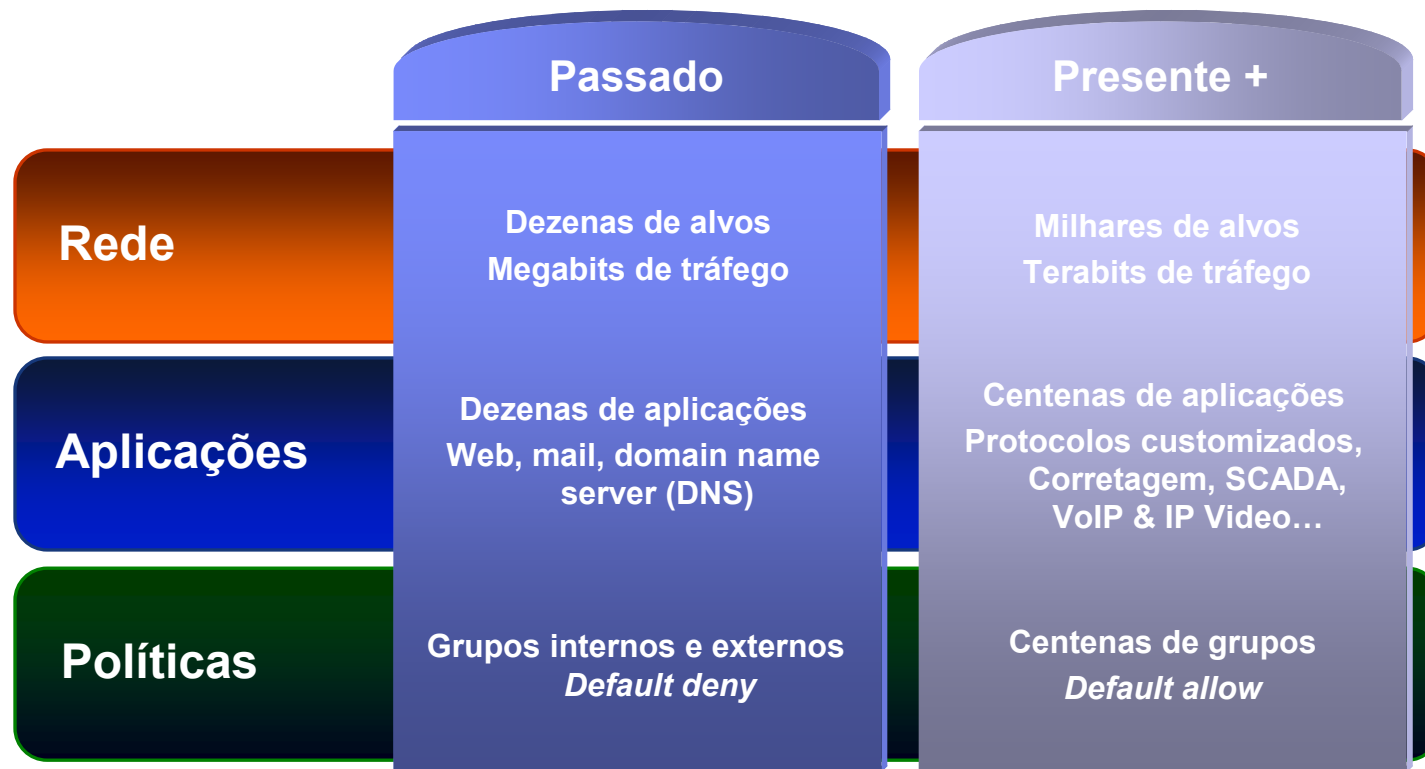


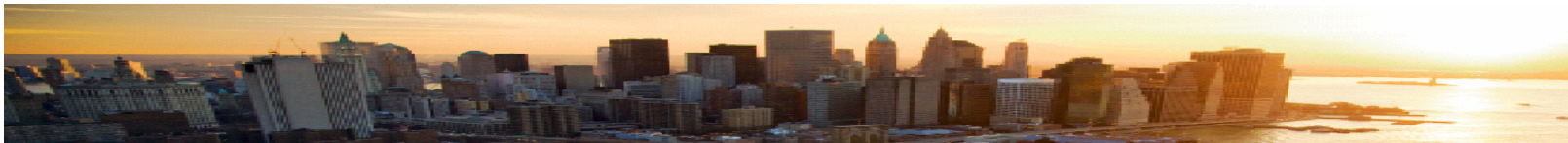
IBM Security Forum
Soluções para um ambiente seguro

Redes 10 Gbps



Tendência: Rede de alto-desempenho (1)





Tendência: Rede de alto-desempenho (2)

“Rede MetroEthernet da Brasil Telecom será implementada pela Alcatel-Lucent”

(<http://www.telecomonline.com.br>)

“Grupo AES renova aposta em Metro Ethernet”

(<http://www.abranet.org.br>)

“RNP implementa rede metro Ethernet da AES Com no RJ”

(<http://www.ipnews.com.br>)

“Campus Party 2009 abrigará 6 mil participantes e terá conexão de 10 Gbps”

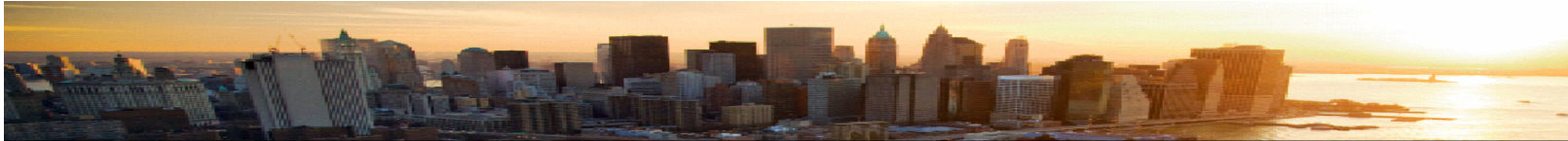
(<http://idgnow.uol.com.br>)

IBM Security Forum
Soluções para um ambiente seguro



IBM Security Forum
Soluções para um ambiente seguro

Padrões de redes 10 Gbps



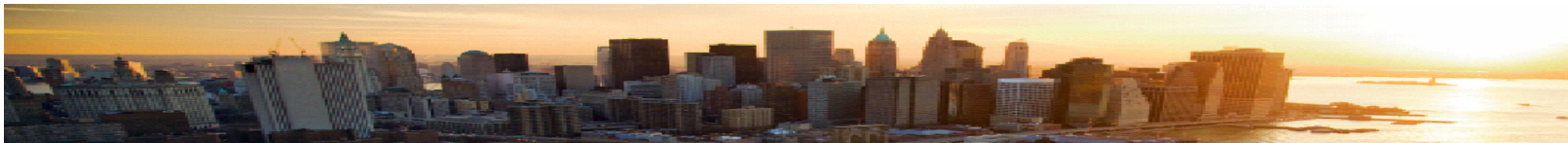
Padrões IEEE

- 802.3ae-2002:
 - 10GBASE-SR (*Short Range*)
 - MMF (*Multimode Fiber*), 26 m a 82 m
 - OM3 MMF, 200 m
 - 10GBASE-LR (*Long Range*)
 - SMF (*Singlemode Fiber*), 10 km
 - 10GBASE-ER (*Extended Range*)
 - PCS (*Physical Coding Sublayer*), 40 km
 - 10GBASE-LX4
 - MMF (*Multi-mode Fiber*), 240 m a 300 m
 - SMF (*Single-mode Fiber*), 10 km
- 802.3ak-2004:
 - 10GBASE-CX4
 - *Copper twin-ax InfiniBand*, 15 m
- 802.3an-2006:
 - 10GBASE-T
 - *Copper Unshielded Twist Pair*, 100 m
 - *Copper Shielded Twist Pair*, 100 m
- 802.3ap-2007:
 - 10GBASE-KX4 e 10GBASE-KR
 - *Backplane Ethernet*
- 802.3aq-2006:
 - 10GBASE-LRM (*Long Reach Multimode*)
 - MMF (*Multimode Fiber*), 220 m



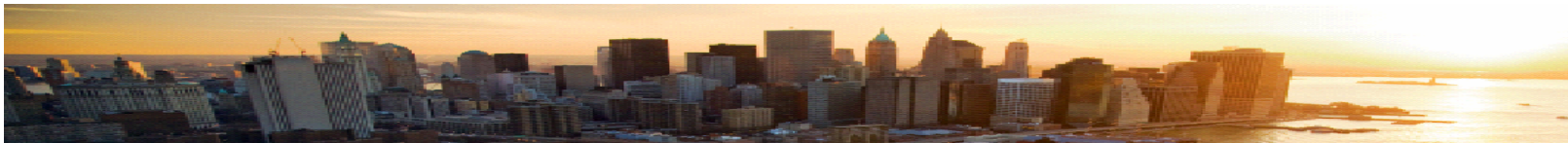
IBM Security Forum
Soluções para um ambiente seguro

Ameaças no *Backbone*



Ameaças no *Backbone* (1)

- **SYNFlood:**
 - Centenas de códigos.
- **UDP Bomber:**
 - Centenas de códigos.
- **BGP Router Attack Tool:**
 - `brat.c`
- **BGP Test Tools & BGP Password Cracker:**
 - `ciag-bgp-tools-1.00.tar.gz`
- **VoIP & IP Video (DEMO):**
 - `ace-1.4.tar.gz`
 - `ucsniff-2.00.tar.gz`
 - `videojak-1.00.tar.gz`
- **MPLS Label Brute-forcer:**
 - `mpls-lbf.c`
- **MPLS Sniffer and Packet Forwarder:**
 - `mpls-fwd.c`
- **DNS Cache Poisoning (DEMO):**
 - `baliwicked_host.rb`
 - `h0dns_spoof.c`
 - `dns_mre-v1.0.tar.gz`



Ameaças no *Backbone* (2)

▪ Cisco:

- IOS FTP Server Multiple Vulnerabilities (Buffer Overflow);
- CVE-2004-0230;
- CVE-2006-3906;
- CVE-2008-0960;
- CVE-2008-1447;
- Etc.

▪ Juniper:

- CVE-2004-0230;
- CVE-2007-6372;
- CVE-2008-0960;
- CVE-2008-1447;
- Etc.

▪ Nortel:

- CVE-2008-0960;
- CVE-2008-1447;
- Etc.

▪ Lucent:

- Multiple Router UDP Port 9 Information Disclosure;
- Brick Spoofed Address Communication Denial Of Service;
- CVE-2008-1447;
- Etc.

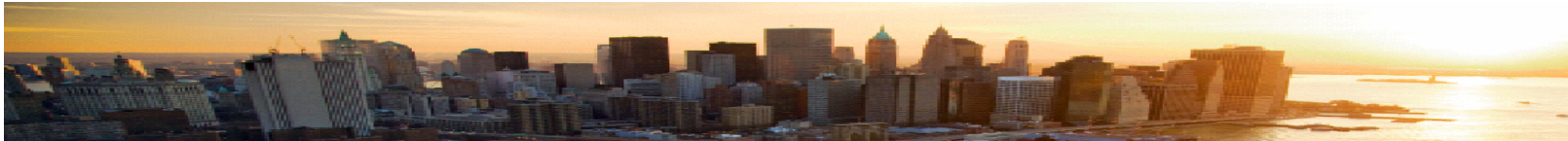
▪ Outros:

- Vulnerabilidade não é privilégio apenas da:
 - Cisco, Juniper, Nortel e Lucent.



IBM Security Forum
Soluções para um ambiente seguro

Exemplos do mundo real



http://www.informationweek.com/shared/printableArticle.jhtml?articleID=202101781 - Windows Internet Explorer

http://www.informationweek.com/shared/printableArticle.jhtml;jsessionid=ANELGVKDEJMGCSNDLPSKHOCJUNN2JVN?articleID=202101781

File Edit View Favorites Tools Help

http://www.informationweek.com/shared/printableAr...

Introducing IBM® LotusLive™ Engage
Connect. Collaborate. And drive business forward. TRY IT NOW IBM

InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

Interview With A Convicted Hacker: Robert Moore Tells How He Broke Into Routers And Stole VoIP Services

On his way to federal prison, the 23-year-old hacker says breaking into computers at telecom companies and major corporations was "so easy a caveman could do it."

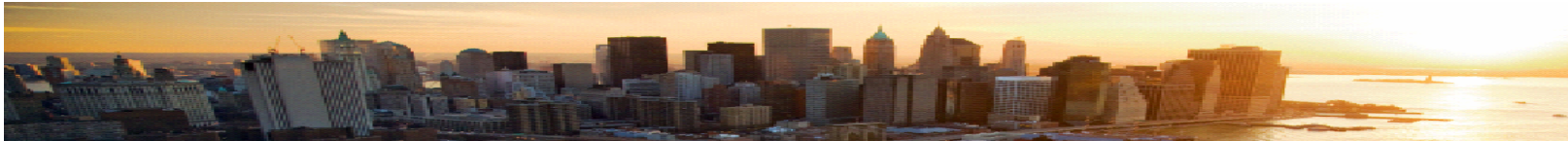
By Sharon Gaudin, [InformationWeek](#)
Sept. 26, 2007
URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=202101781>

Convicted hacker Robert Moore, who is set to go to federal prison this week, says breaking into 15 telecommunications companies and hundreds of businesses worldwide was incredibly easy because simple IT mistakes left gaping technical holes.

Moore, 23, of Spokane, Wash., pleaded guilty to conspiracy to commit computer fraud and is slated to begin his two-year sentence on Thursday for his part in a [scheme to steal voice over IP services](#) and sell them through a separate company. While prosecutors call co-conspirator Edwin Pena the mastermind of the operation, Moore acted as the hacker, admittedly scanning and breaking into telecom companies and other corporations around the world.

Done

IBM Security Forum
Soluções para um ambiente seguro



Alert Details - Security Center - Cisco Systems - Windows Internet Explorer

http://tools.cisco.com/security/center/viewAlert.x?alertId=16502

Cisco Shellcode

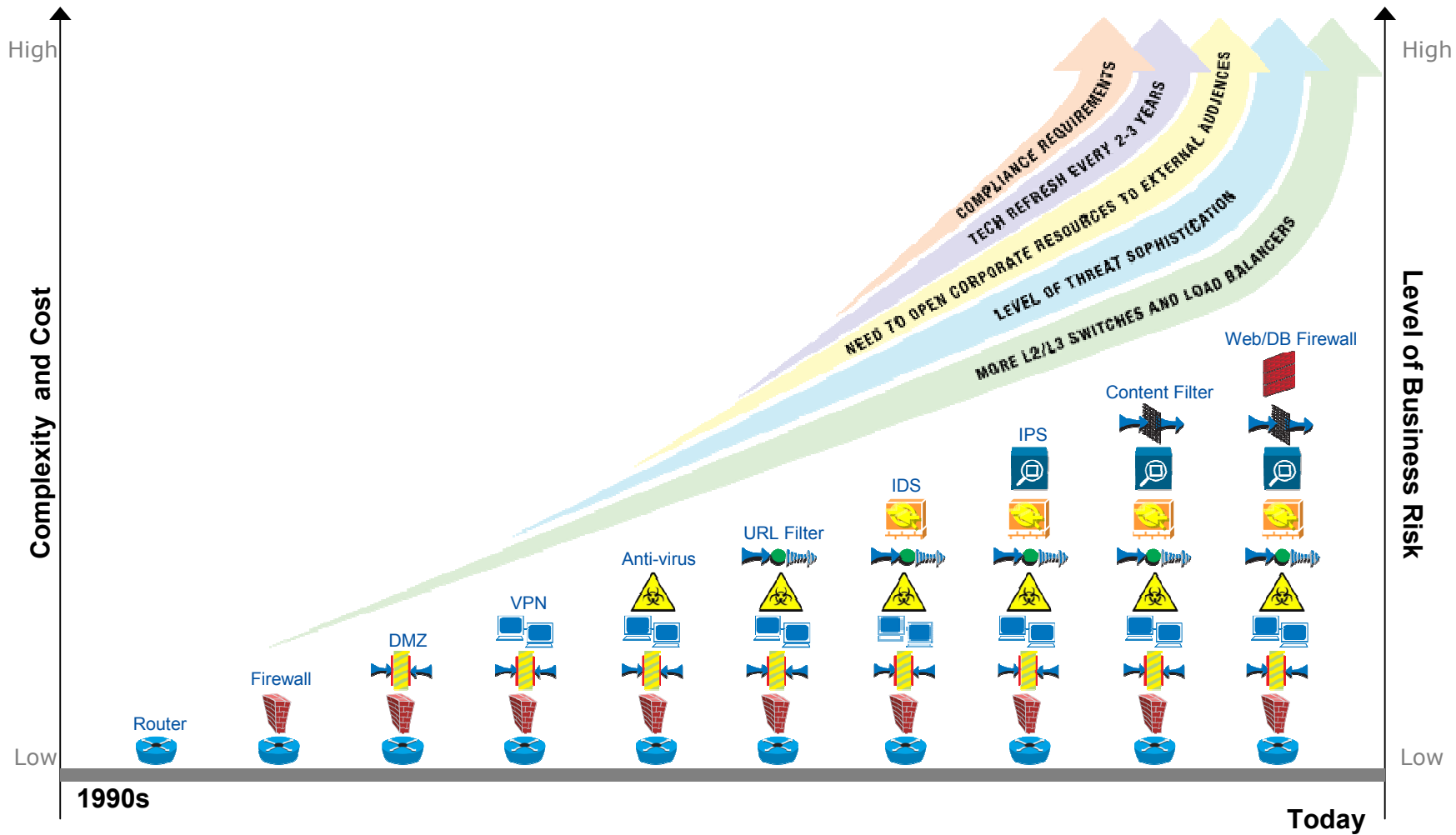
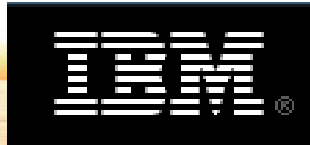
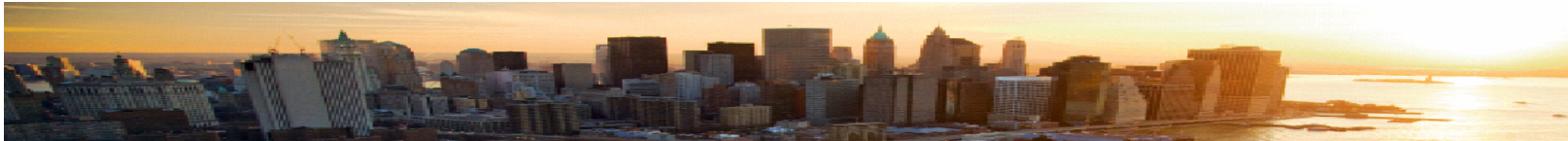
Security Center

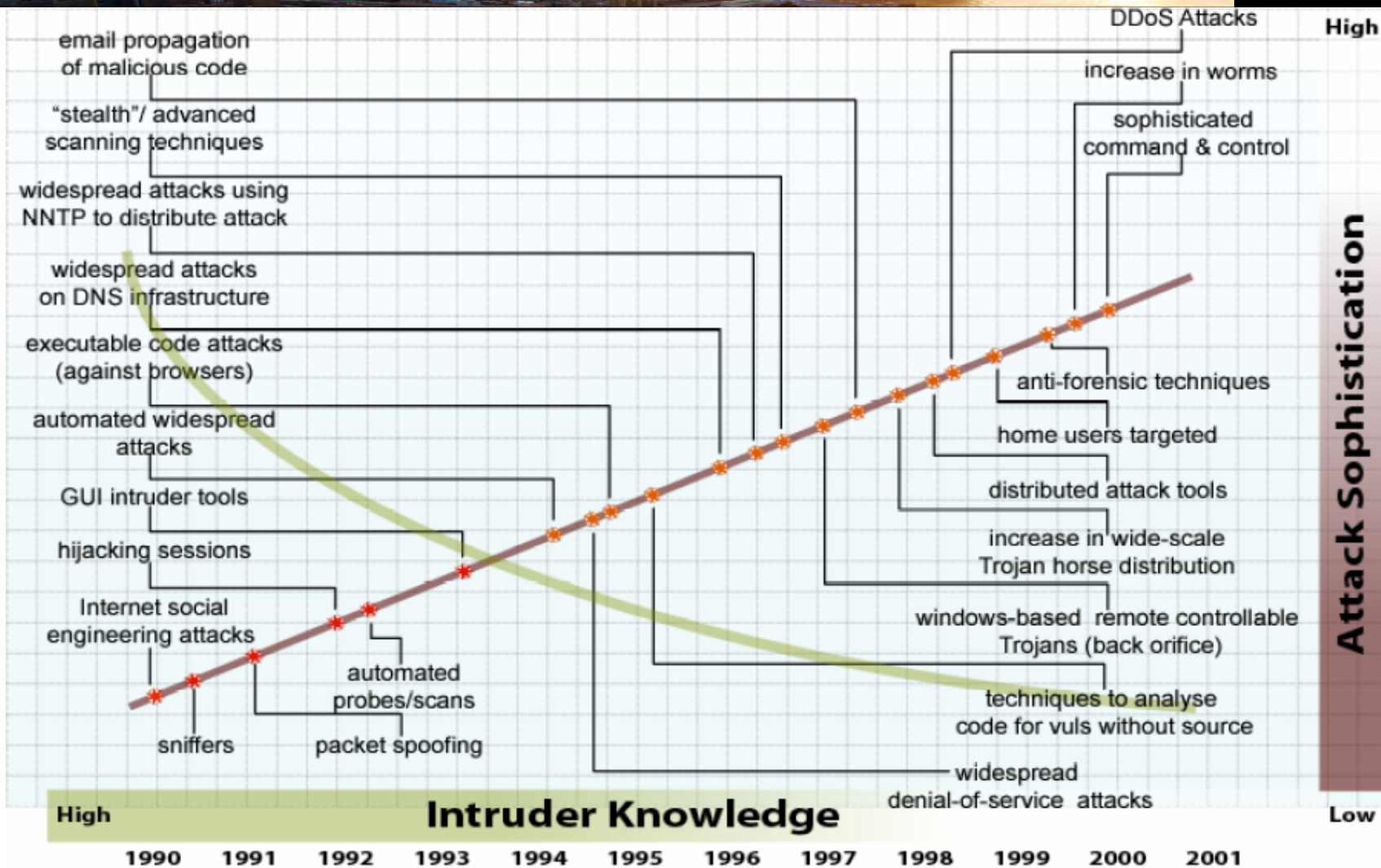
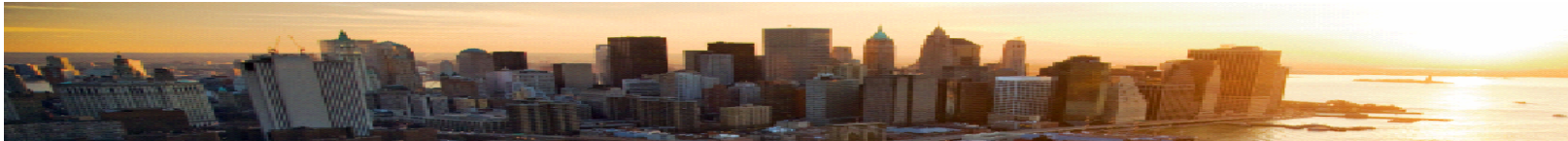
Shellcode for Multiple Cisco IOS Systems Released

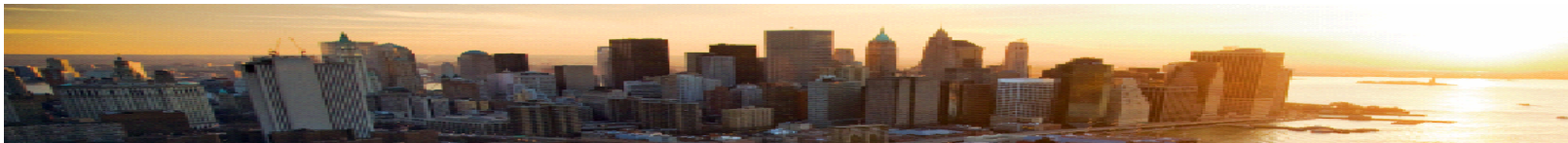
SECURITY ACTIVITY BULLETIN

Title:	IntelliShield: Security Activity Bulletin		
ID:	16502	Urgency:	U
Severity:	1	Credibility:	C
Released:	August 21, 2008 06:16 PM EDT	Severity:	M
Updated:	August 21, 2008 06:16 PM EDT		
Not Available:			

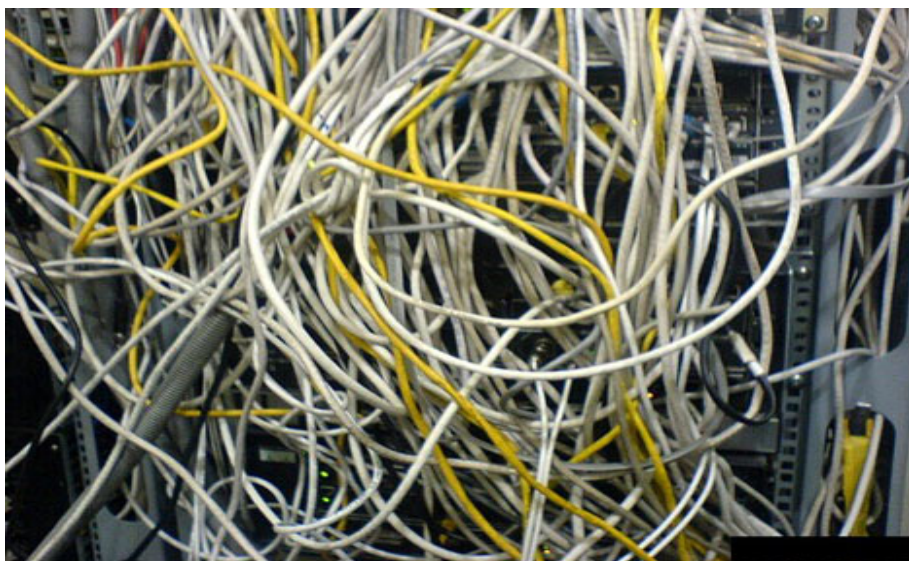
Done







Conseguimos trabalhar assim?

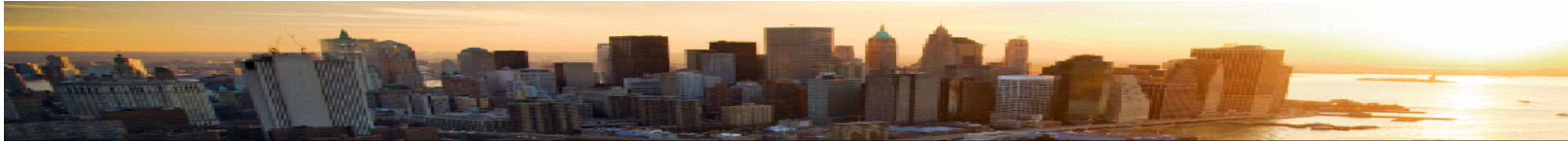


IBM Security Forum
Soluções para um ambiente seguro



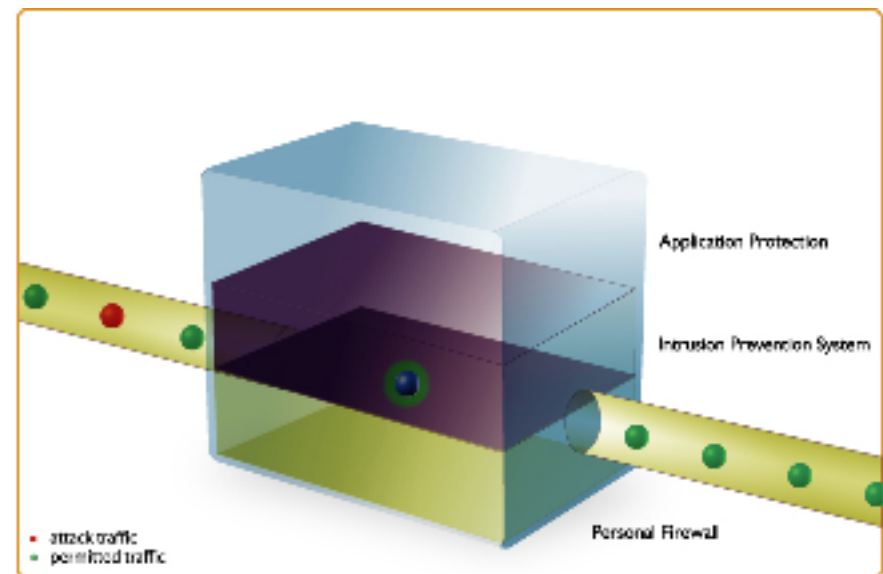
IBM Security Forum
Soluções para um ambiente seguro

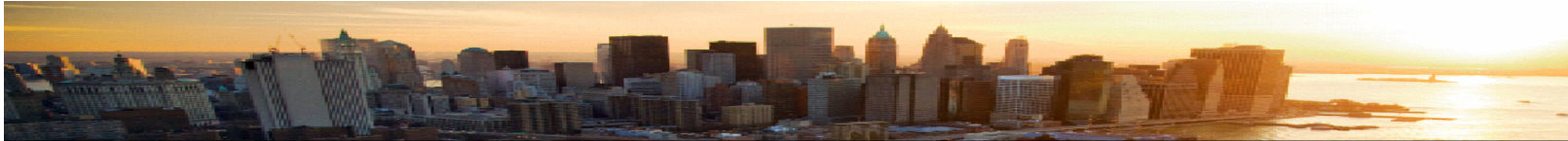
Intrusion Prevention System



Conceito de IPS

- Todo ataque possui duas variáveis comuns:
 - ORIGEM
 - Invasor / Atacante;
 - DESTINO
 - Vítima / Alvo.
- O IPS está localizado, conceitual e estrategicamente, entre estes dois pontos.





Análise de Protocolo

- Análise de Protocolos é a utilização de *Software* e *Hardware* para capturar, decodificar, interpretar e reagir ao conteúdo de pacotes de dados enquanto eles trafegam em uma rede.
- Benefícios:
 - Maior precisão;
 - Menos falso positivos;
 - $\approx 0\%$ de falso negativos;
 - Mais robustez e rapidez na análise.
- *Protocol Analysis Module*TM.



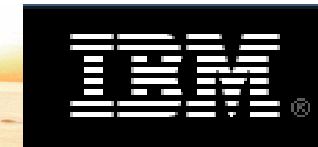
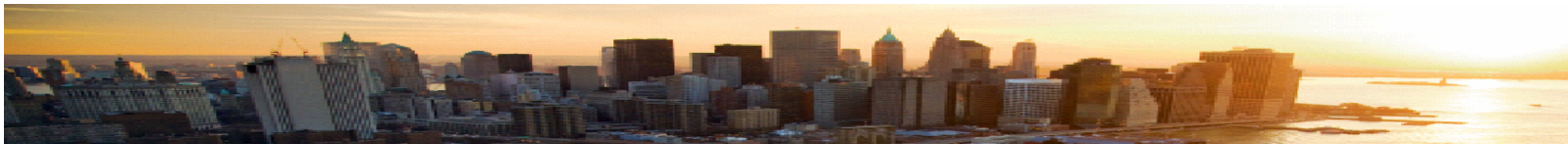
Protocol Analysis Module™

- Incríveis **204** protocolos, assim como formatos de dados associados, são reconhecidos e decodificados pelo PAM™ atendendo camadas do modelo OSI.
- Mais de **2.800** algoritmos, proporcionando proteção para eventos de segurança únicos.
- Oferece **20** métodos de detecção, com milhares de algoritmos inclusos.
- Os métodos são utilizados em conjunto, aumentando drasticamente a eficiência da detecção.
- O PAM™ é a primeira e única tecnologia da indústria de segurança a ser incorporada em agentes de rede, servidores e estações de trabalho, assim como *Appliances*.
- Atendendo inclusive a redes de alto-desempenho, tais como: **1 Gbps & 10 Gbps**.



IBM Security Forum
Soluções para um ambiente seguro

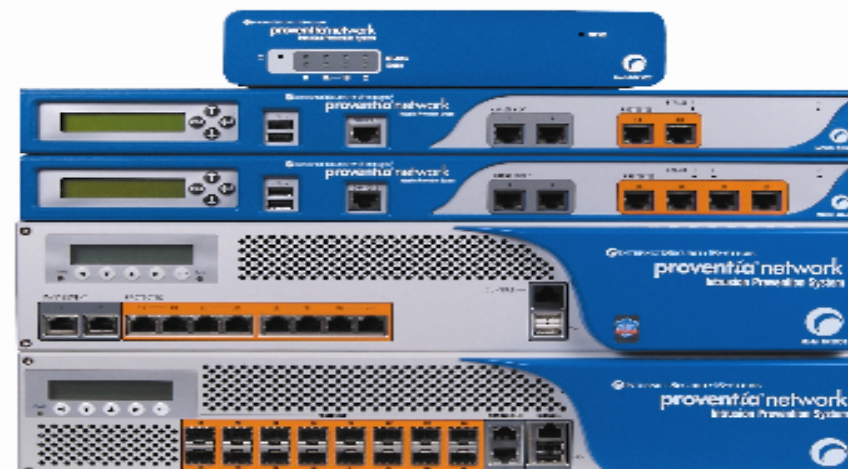
IBM Proventia® Network IPS



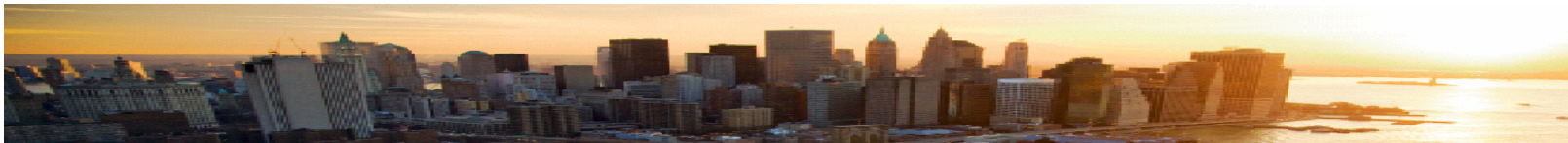
IBM Proventia® Network IPS (1)



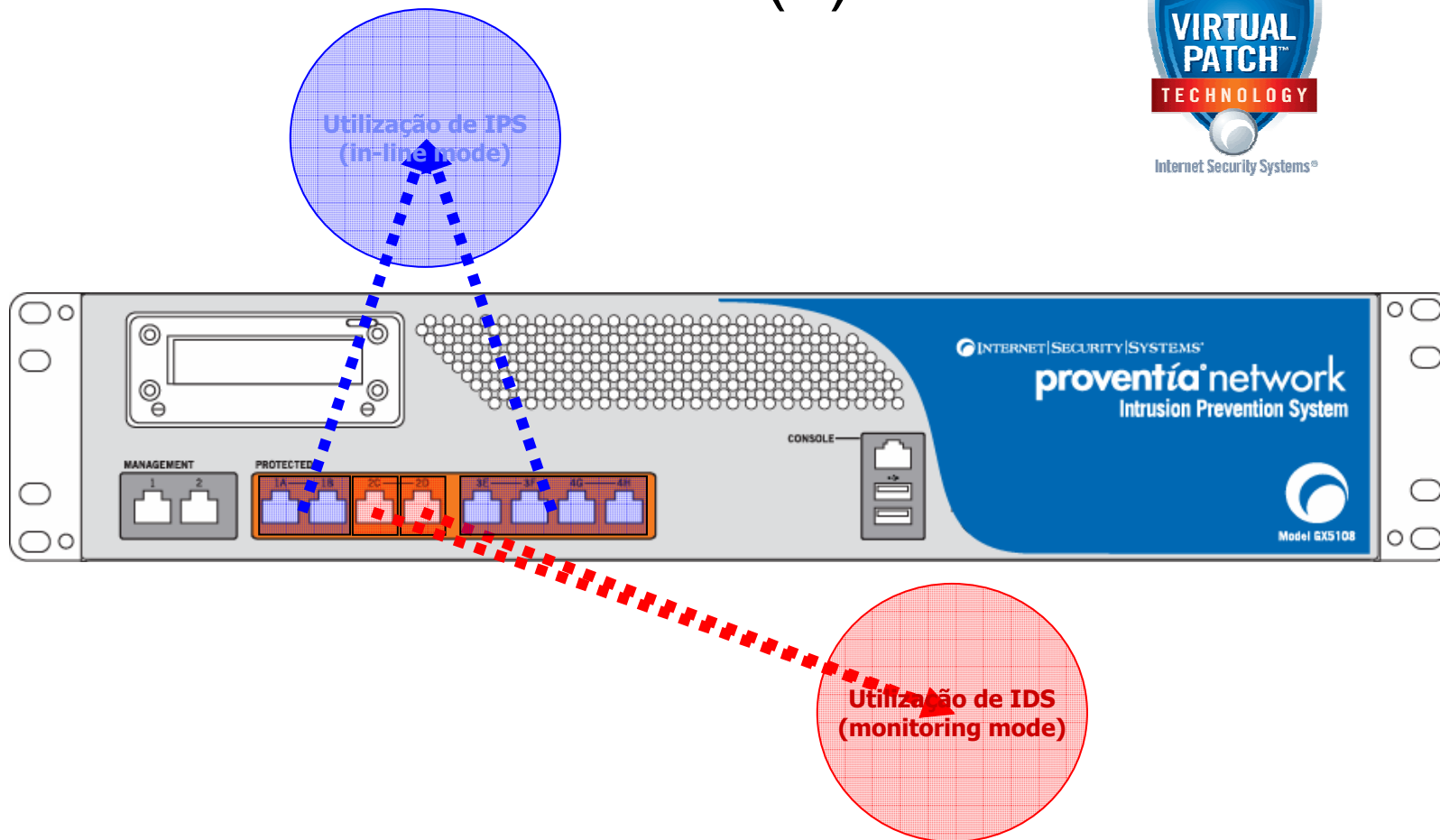
- Impede que sistemas vulneráveis sejam invadidos.
- Proteção:
 - VoIP;
 - SCADA;
 - GTP;
 - Backbones;
 - Servidores;
 - Perímetros;
 - Etc.

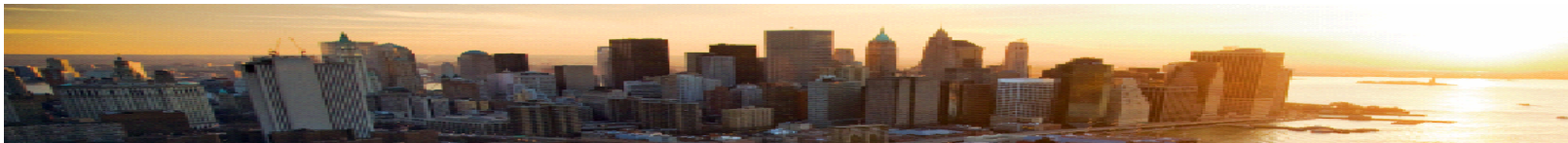


IBM Security Forum
Soluções para um ambiente seguro



IBM Proventia® Network IPS (2)

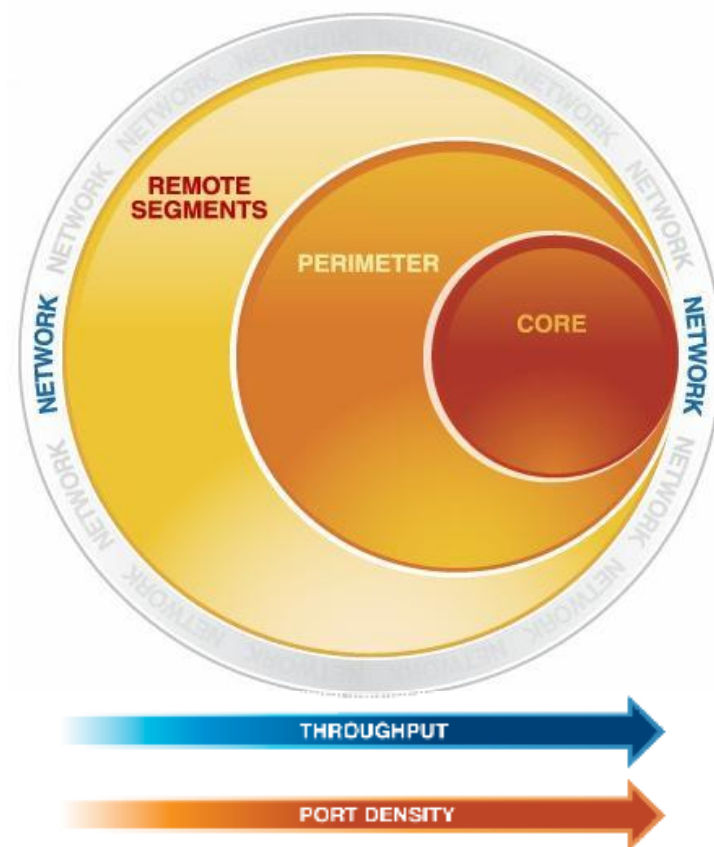




IBM Proventia® Network IPS (3)

GX3002	10 Mbps	2 portas
GX4002	200 Mbps	2 portas
GX4004	200 Mbps	4 portas
GX5008	400 Mbps	8 portas
GX5108	1.2 Gbps	8 portas
GX5208*	2.0 Gbps	8 portas
GX6116*	6.0 Gbps	16 portas

** Equipamentos desenvolvidos para redes de alto-desempenho.*

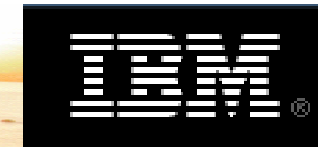
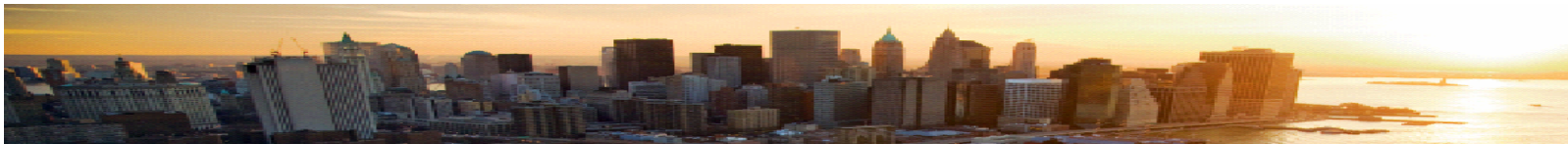


IBM Security Forum
Soluções para um ambiente seguro



IBM Security Forum
Soluções para um ambiente seguro

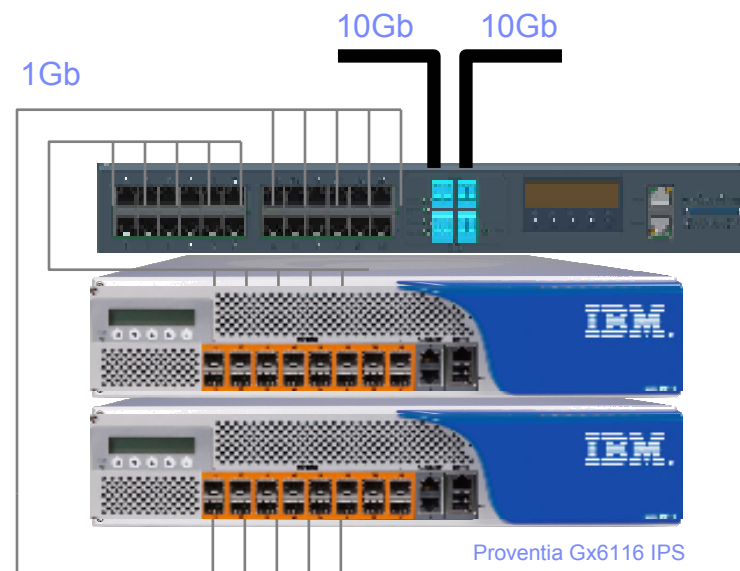
IBM Proventia® Network Security Controller

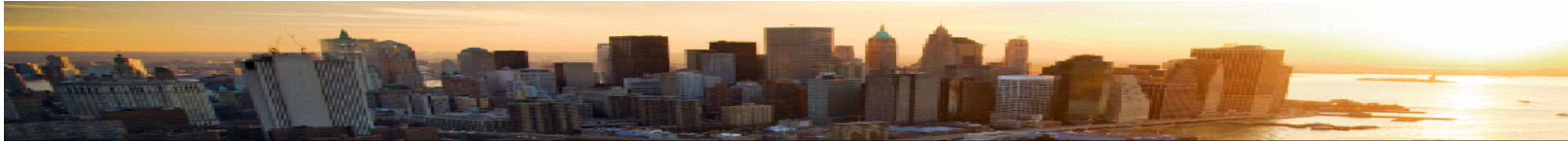


IBM Proventia® Network Security Controller (1)

- Proteção para Redes 10 Gbps:
 - Proteção baseada em vulnerabilidades (*World Class*);
 - Fornece conexão 10 Gbps para equipamentos com interfaces 1 Gbps (GX6116 & GX5208);
 - Combina o poder de múltiplos equipamentos para proteção 10 Gbps integral.
- Estende a vida útil de um investimento prévio:
 - Re-disposição de equipamentos GX6116 & GX5208 em Redes 10 Gbps.
- Entrega funcionalidade integral de *Bypass*:
 - *Bypass/Switching* ativo para não interrupção da Rede;
 - *Bypass/Switching* passivo no caso de queda de energia;
 - Não necessita de compra / aquisição separada de equipamento de *Bypass*.

IBM Proventia® Network Security Controller
(Conectividade 10Gbps com *Bypass* Integrado)

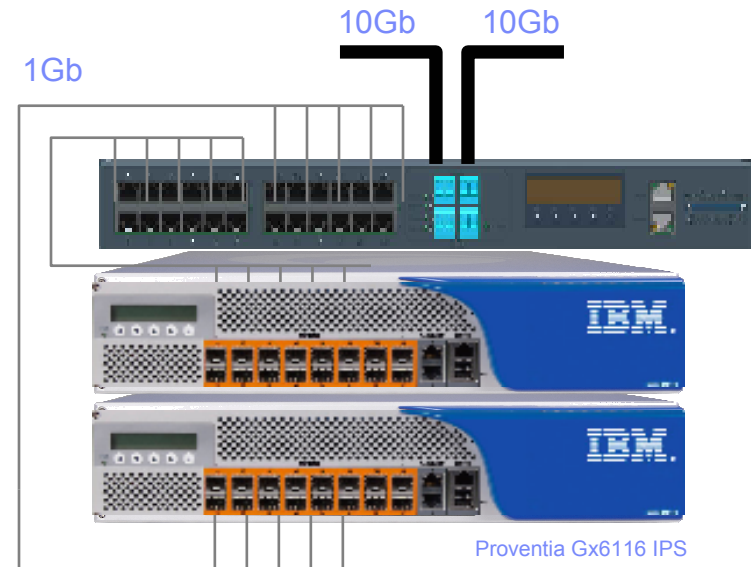




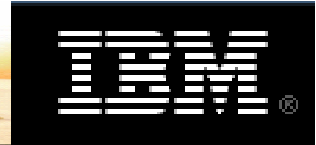
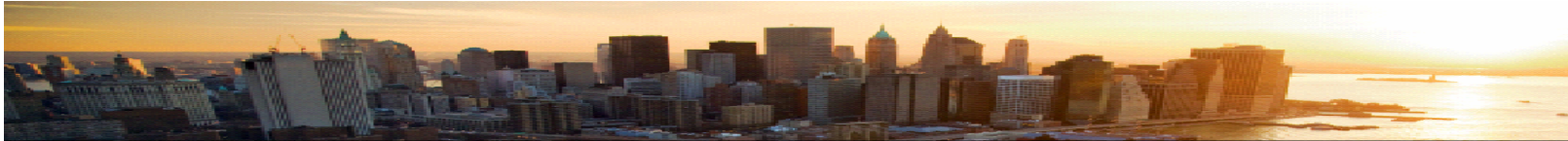
IBM Proventia® Network Security Controller (2)

- Aglomerado de 10 Gbps:
 - Quatro (04) NIC 10 GbE;
 - Dois (02) segmentos 10GbE.
- Agregar / Segregar 4 x 10Gbps:
 - 24 x 1Gb *Copper Twist Pair*;
 - 24 x 1GbE *SR / LR Fiber*;
 - 24 x 1GbE *Built-in Bypass*.
- A mesma proteção preemptiva / preventiva líder de mercado no *Backend*.

IBM Proventia® Network Security Controller
(Conectividade 10Gbps com *Bypass* Integrado)



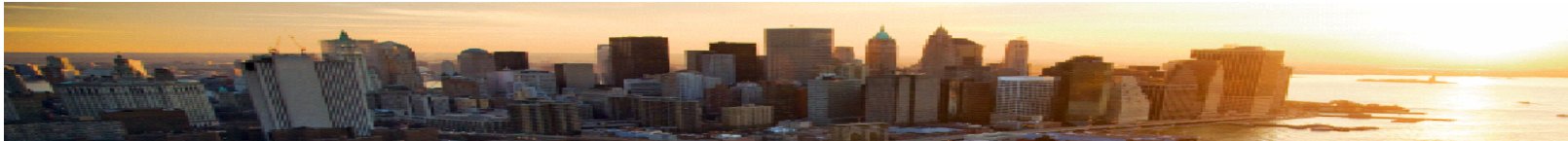
IBM Security Forum
Soluções para um ambiente seguro



IBM Proventia® Network Security Controller (3)



IBM Security Forum
Soluções para um ambiente seguro



IBM Proventia® Network Security Controller (4)

Status Page

IBM Proventia Network Security Controller Language selection: English | Logout

- Home
- Status
- Segment Setting
- Heartbeat Frame
- Segments Configuration Management
- Management Port
- Email Notifications
- SNMP Settings
- Advanced
- Users
- Backup/Restore
- Firmware Update

Status

System	
Product Name:	Proventia NSC
Product ID:	0x41
Hardware Revision:	1
Firmware Version:	NBCv1.0
Management IP:	192.168.1.111
Physical Address (MAC):	00:0C:BD:00:00:03
Email Notifications:	Disable (Don't Send)

Power Supply Status	
Power A:	● Present
Power B:	● Not Present

Segment A	
State:	● Active
Module Media Type:	RJ-RJ

Segment B	
State:	● Bypass
Module Media Type:	RJ-RJ

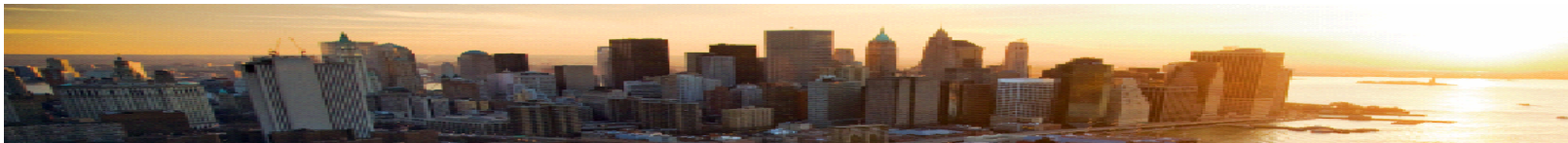
Segments Settings

Done



IBM Security Forum
Soluções para um ambiente seguro

**IBM Proventia® Network IPS for
Crossbeam®**

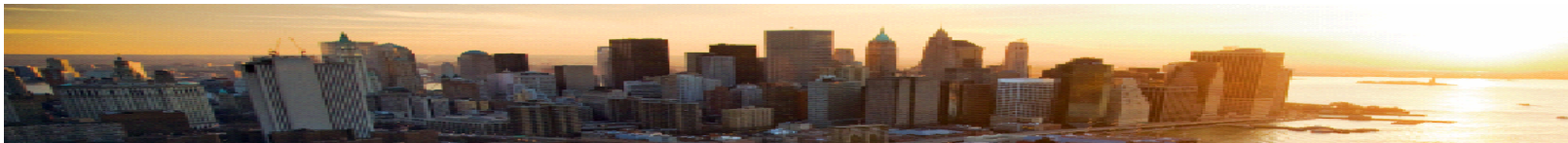


IBM Proventia® IPS for Crossbeam® (1)

- Crossbeam® Security Platform:
 - Baseado em chassi: *Next-generation Security Platform*;
 - 100% integrado com soluções líderes de segurança (*WEB Filtering, Firewall, Network IPS, etc*), entre elas IBM Proventia® Network IPS;
 - Desenvolvido para alto-desempenho, alta-disponibilidade e escalabilidade.
- IBM Internet Security Systems:
 - A mesma proteção preemptiva / preventiva líder de mercado no *Backend*;
 - Proteção baseada em vulnerabilidades (*World Class*).



IBM Security Forum
Soluções para um ambiente seguro

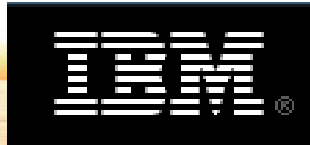
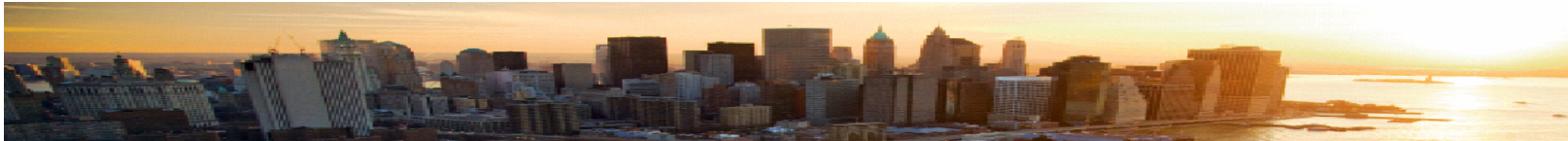


IBM Proventia® IPS for Crossbeam® (2)

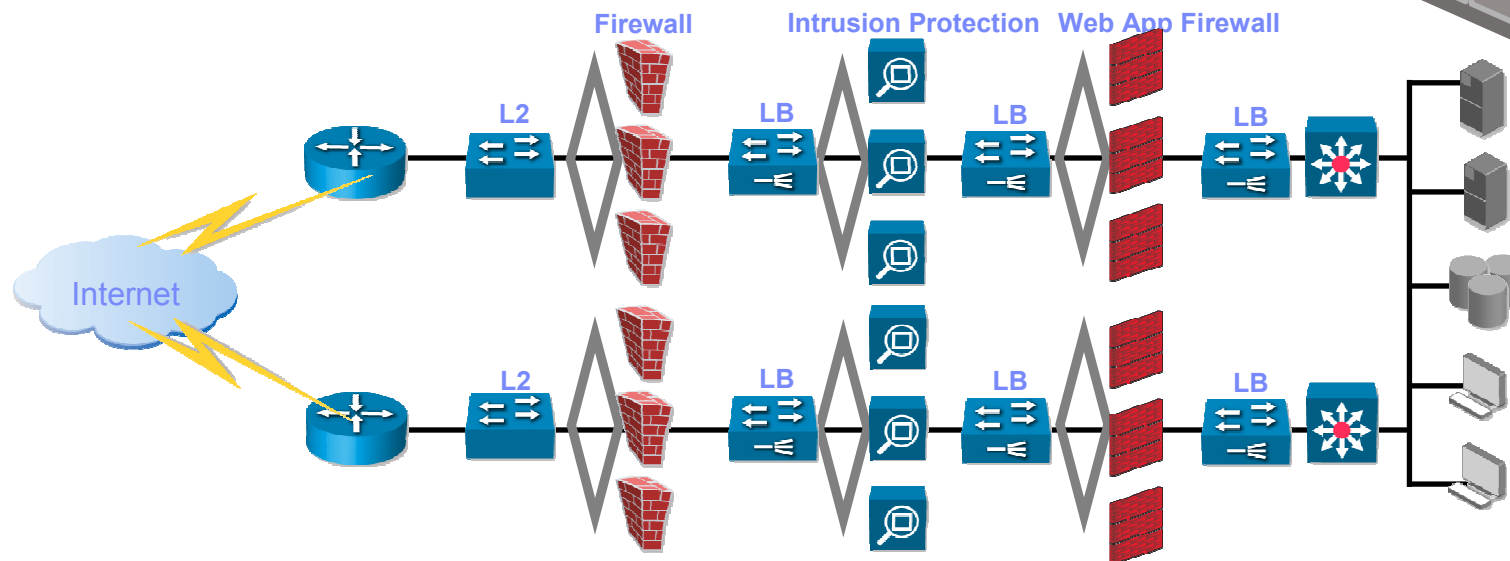
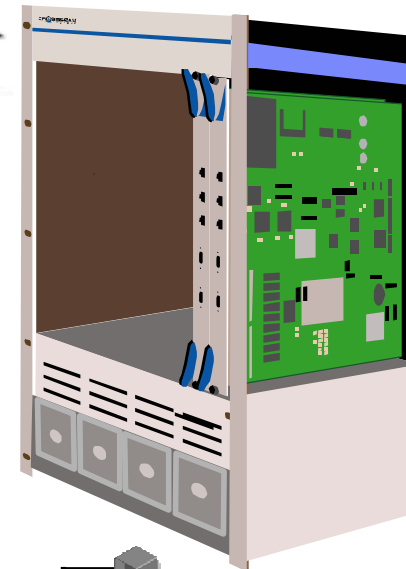
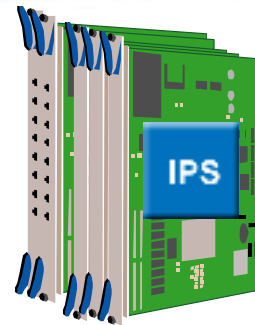
- Virtualização direcionada para:
 - Consolidação;
 - Desempenho.
- Network Processor Modules:
 - Políticas de *Switch* e *Load-Balance*.
- Application Processor Modules:
 - Aplicações de segurança virtualizadas.
- Control Processing Modules:
 - Monitoração de *High-Availability*, *Fail-Over*, *Self-Healing*.



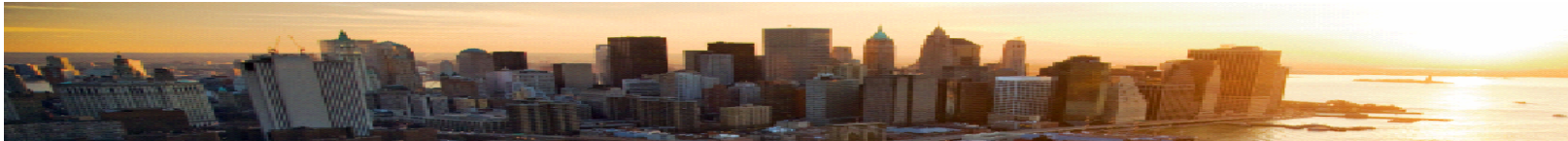
IBM Security Forum
Soluções para um ambiente seguro



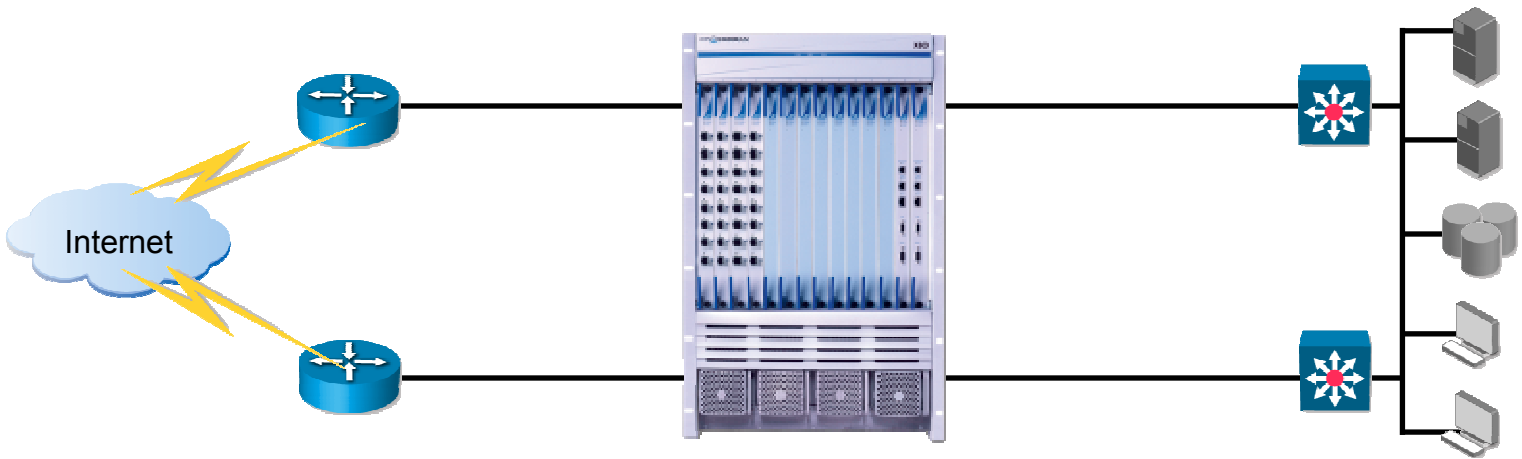
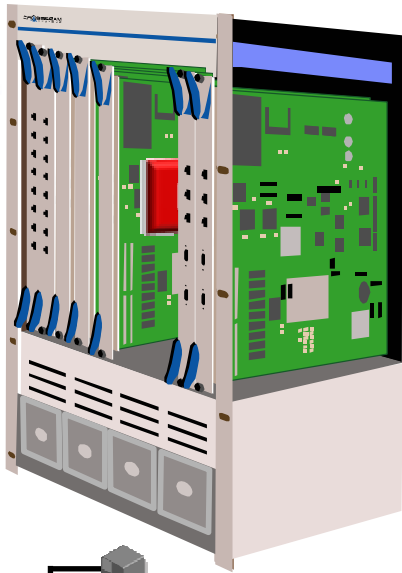
CROSSBEAM
SYSTEMS



IBM Security Forum
Soluções para um ambiente seguro



CROSSBEAM
SYSTEMS

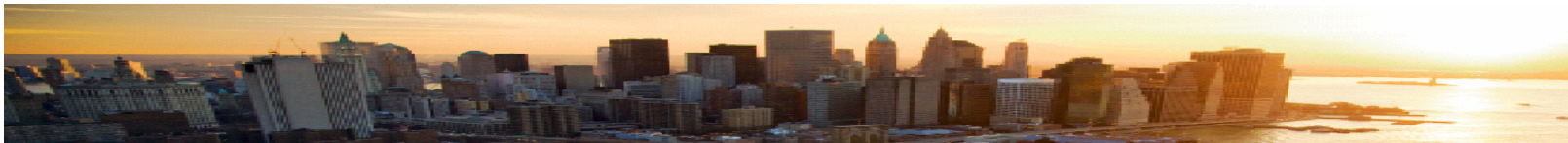


IBM Security Forum
Soluções para um ambiente seguro



IBM Security Forum
Soluções para um ambiente seguro

Perguntas e Respostas



Dúvidas?

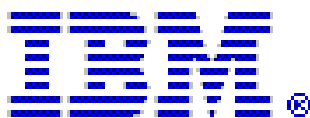


IBM Security Forum
Soluções para um ambiente seguro



IBM Security Forum

Soluções para um ambiente seguro



Nelson Brito

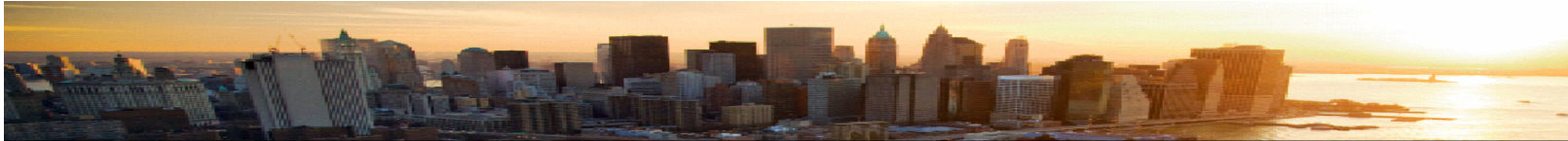
*Senior Security Engineer
Internet Security Systems*

IBM Brasil Ltda.

*Av. Pasteur ,138/146 – Botafogo
Cep: 22290-903 – Rio de Janeiro – RJ – Brasil
Fone 1.: +55 21 2132-5499
Fone 2.: +55 21 8121-1774
nbrito@br.ibm.com
<http://www.ibm.com/br>*

Obrigado!

Aproveitem o resto do evento!



VOCÊ ESTÁ PREPARADO PARA ENFRENTAR A TEMPESTADE DAS REDES DE ALTO-DESEMPENHO!

IBM Security Forum
Soluções para um ambiente seguro

© 2009 IBM Corporation

