IBM Security Forum

Soluções para um ambiente seguro

Proteção de alto-desempenho para *Backbones*

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

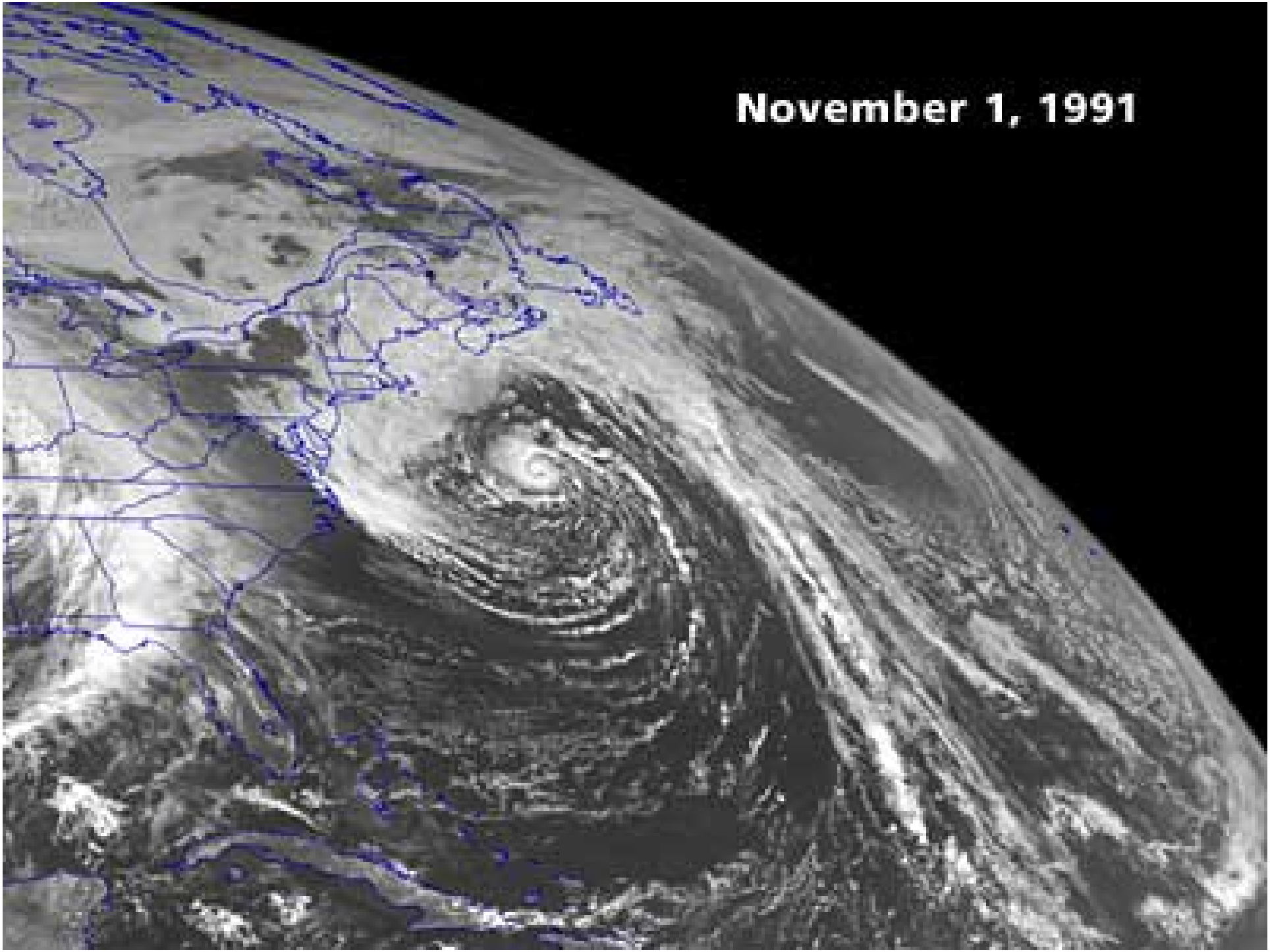
Agenda

- 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

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

IBM Security Forum

Soluções para um ambiente seguro

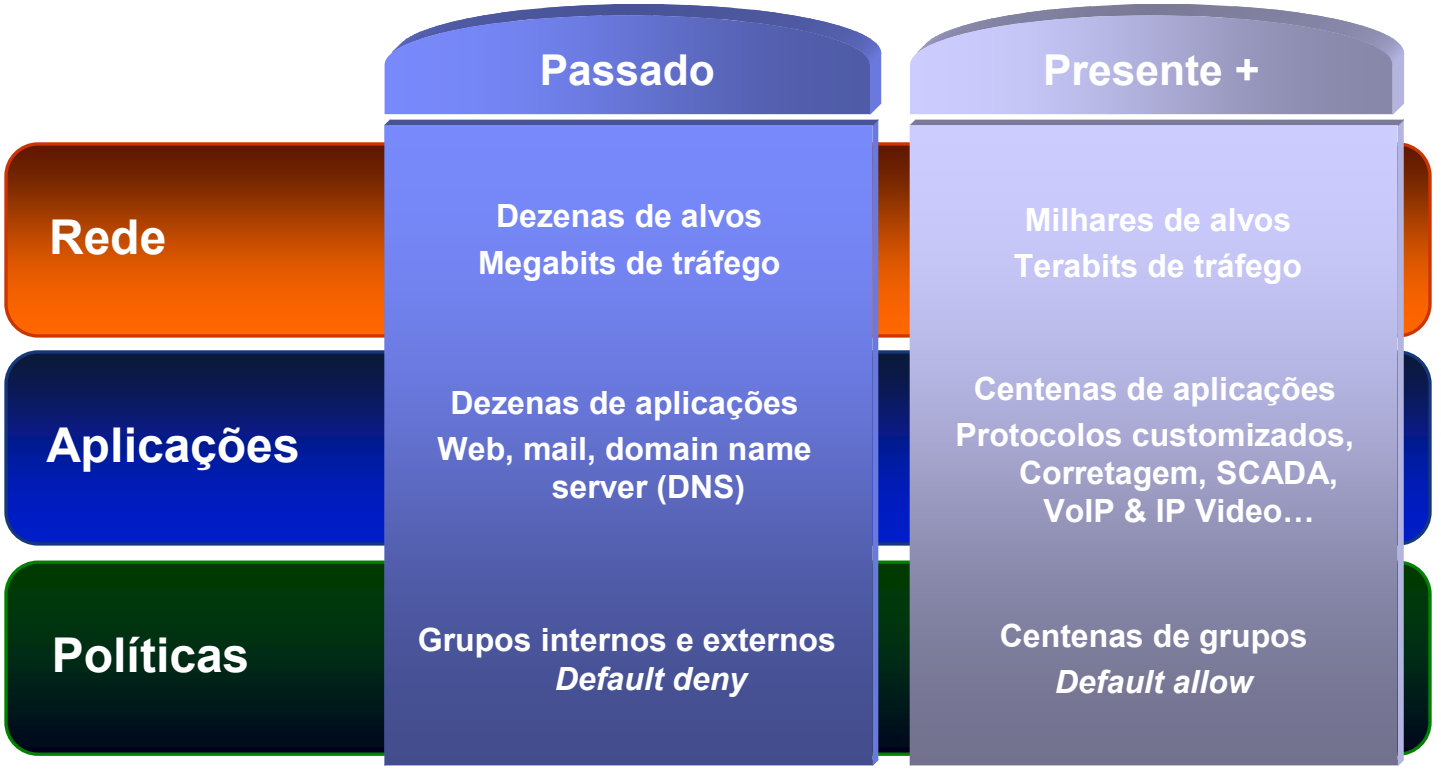

November 1, 1991

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

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.

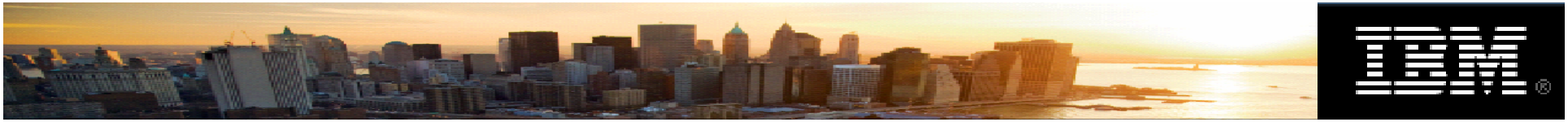
IBM Security Forum

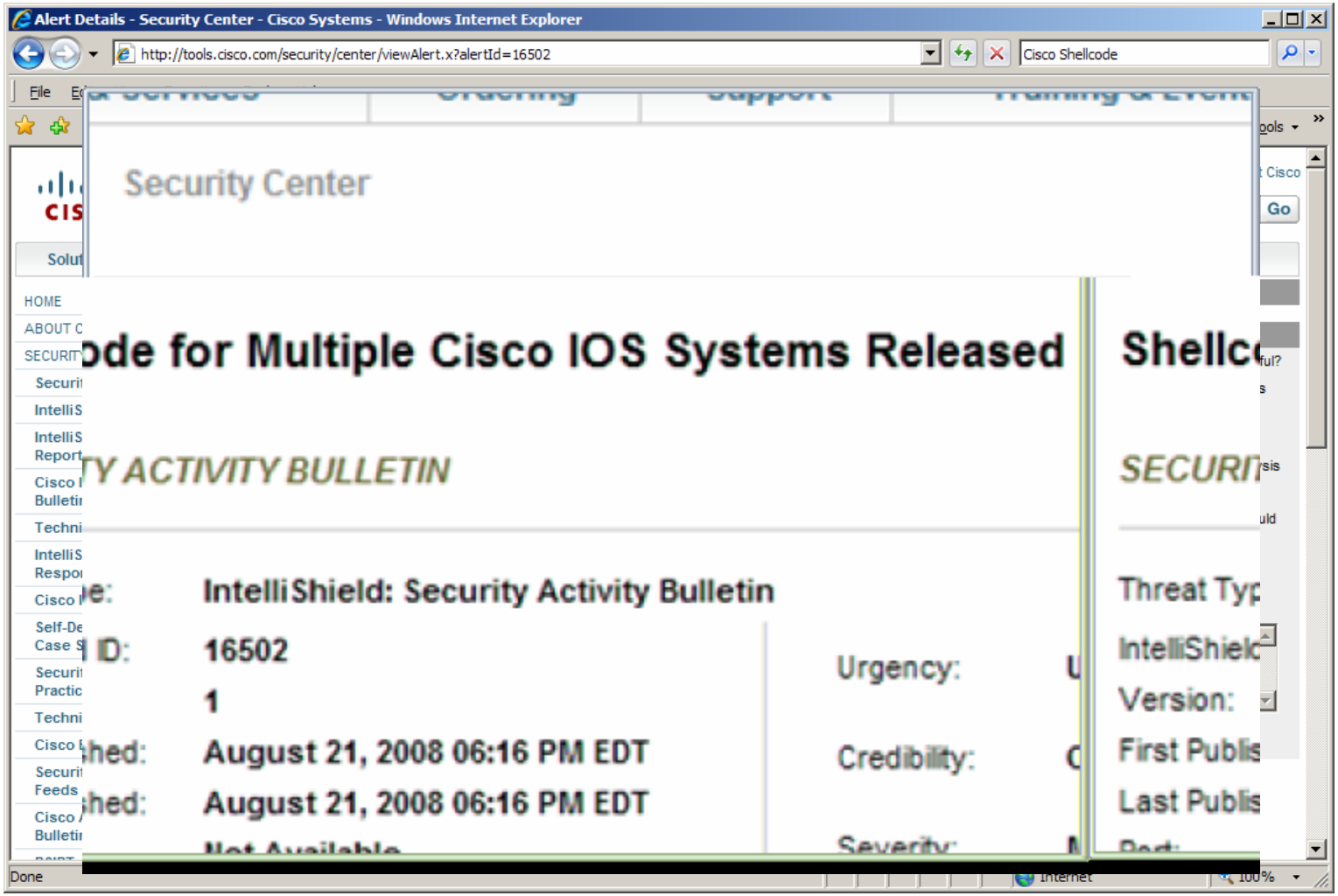
Soluções para um ambiente seguro

Exemplos do mundo real

IBM Security Forum

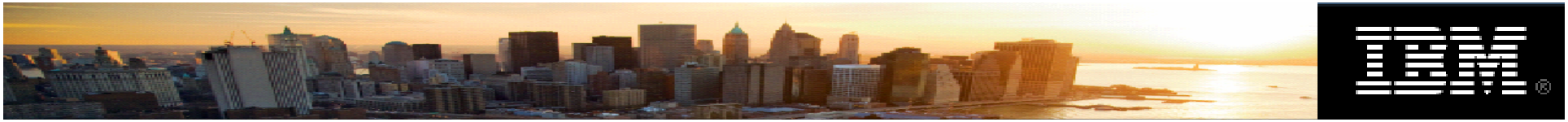
Soluções para um ambiente seguro

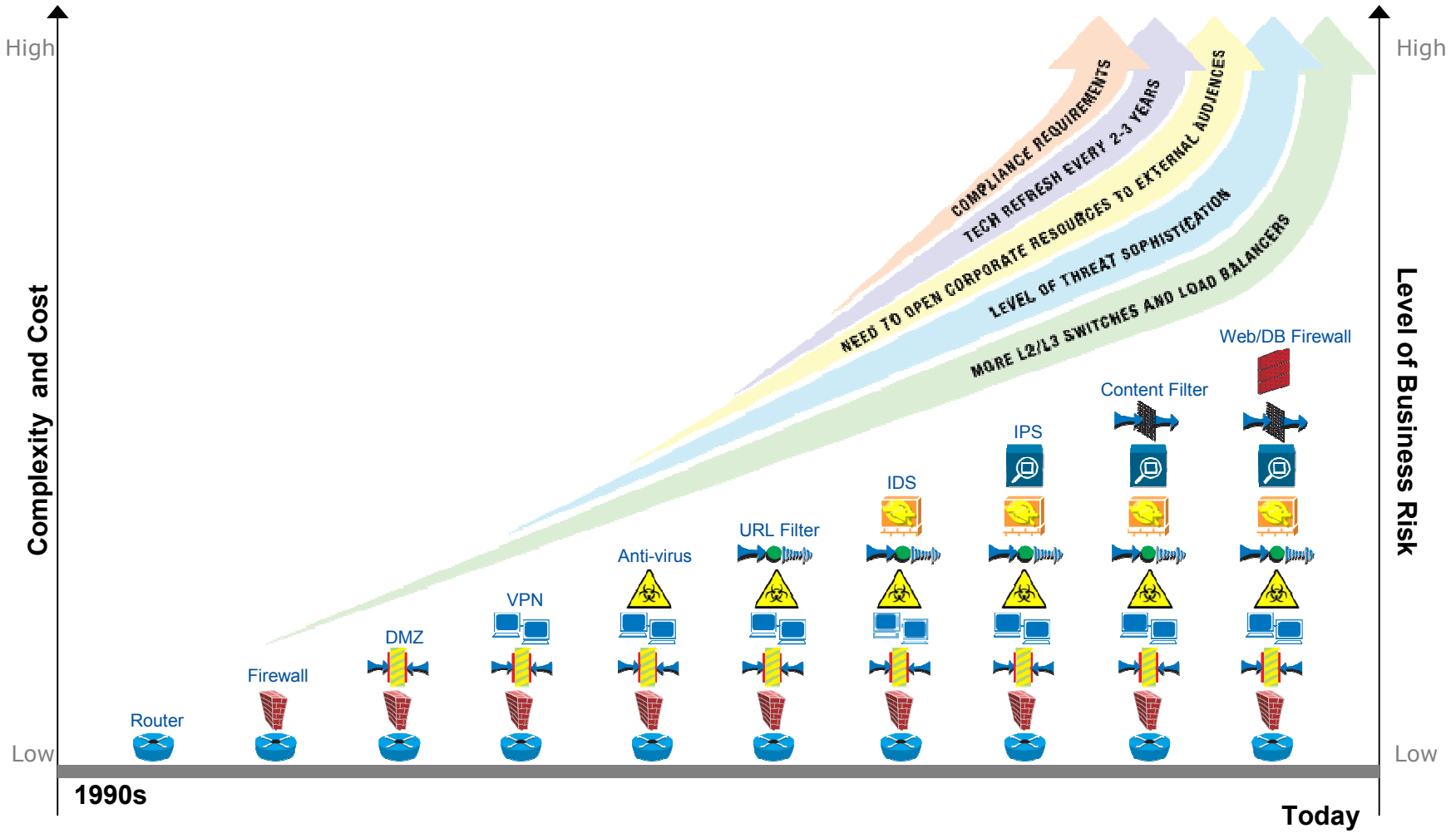




IBM Security Forum

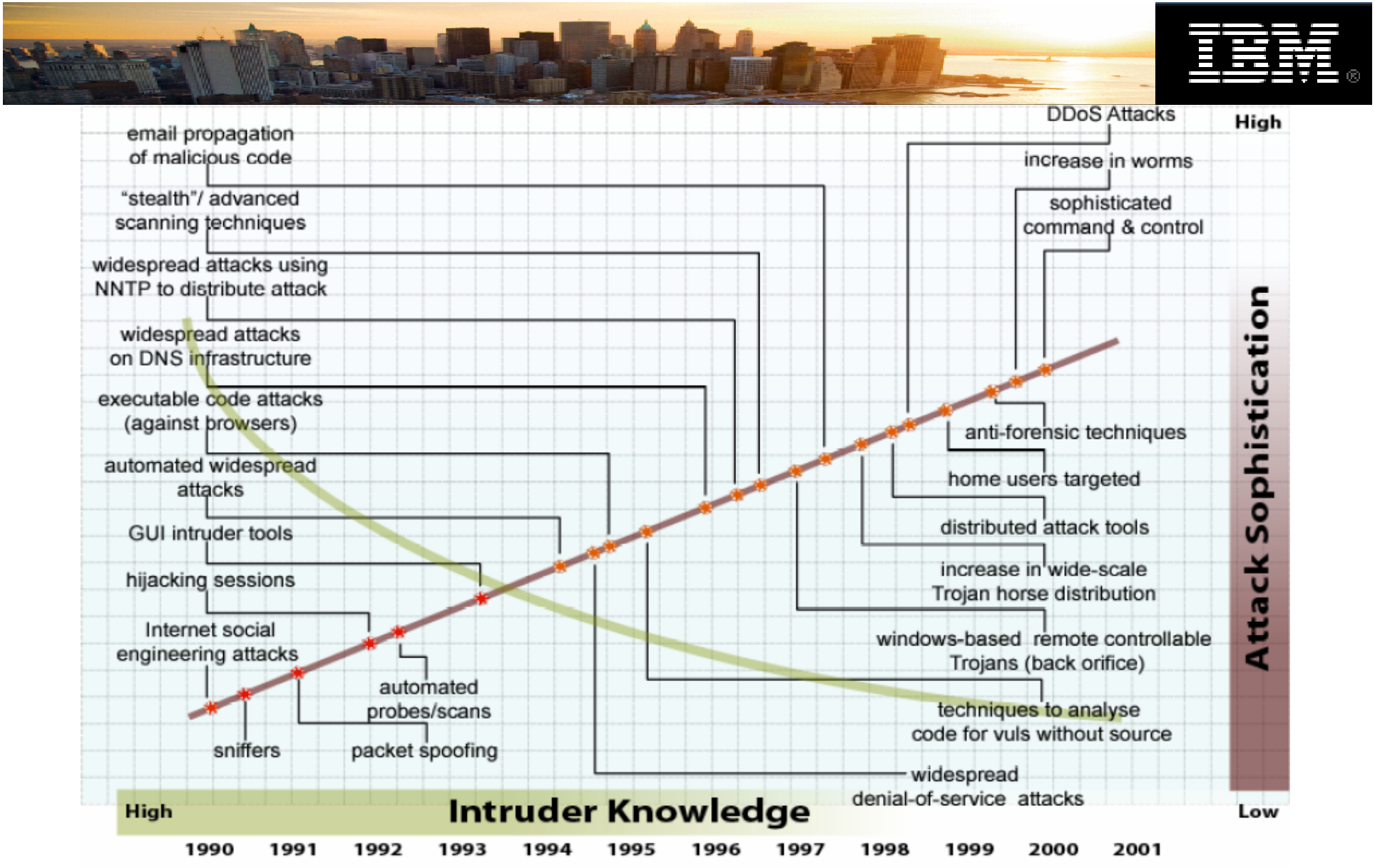
Soluções para um ambiente seguro





IBM Security Forum

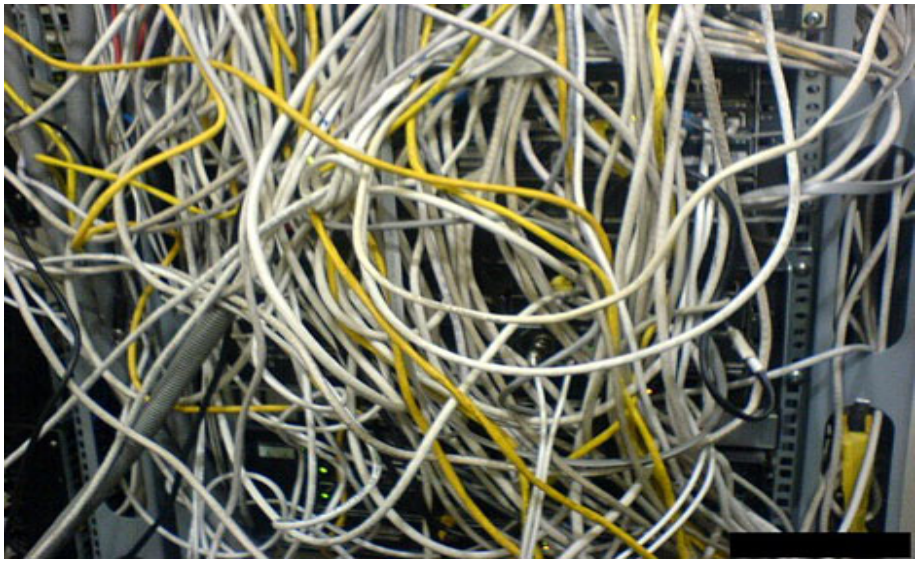
Soluções para um ambiente seguro



IBM Security Forum

Soluções para um ambiente seguro

Conseguimos trabalhar assim?



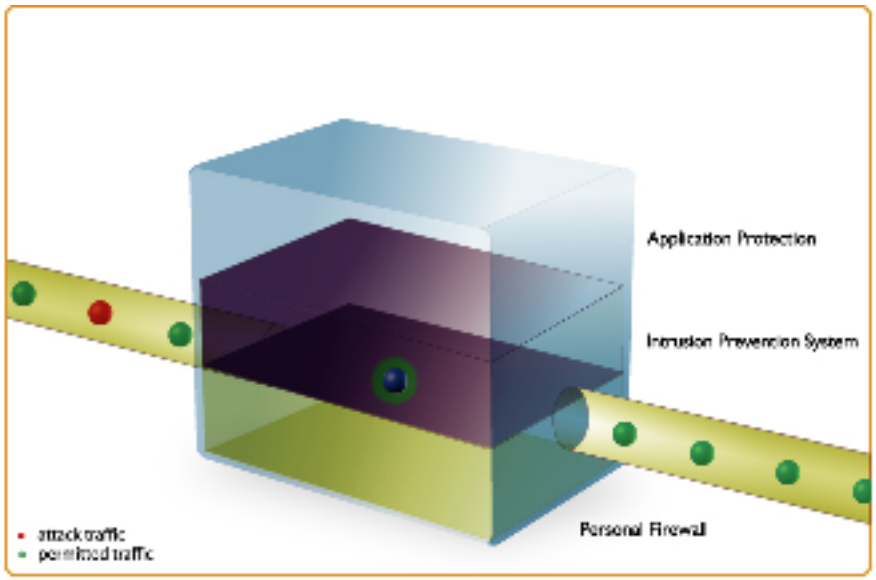
IBM Security Forum

Soluções para um ambiente seguro

Intrusion Prevention System

Conceito de IPS

- Todo ataque possuí 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;
  - ≈ 0% de falso negativos;
  - Mais robustez e rapidez na análise.
- *Protocol Analysis Module*™.

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

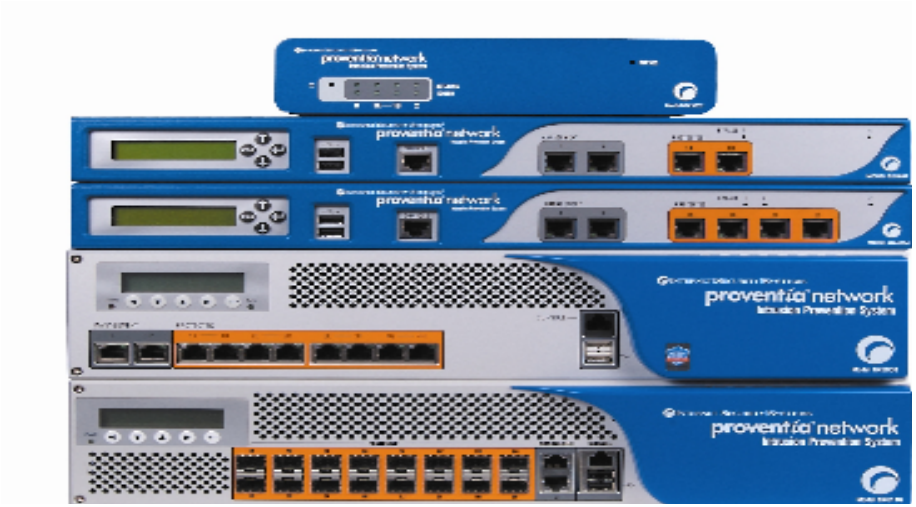
Soluções para um ambiente seguro

IBM Proventía® Network IPS

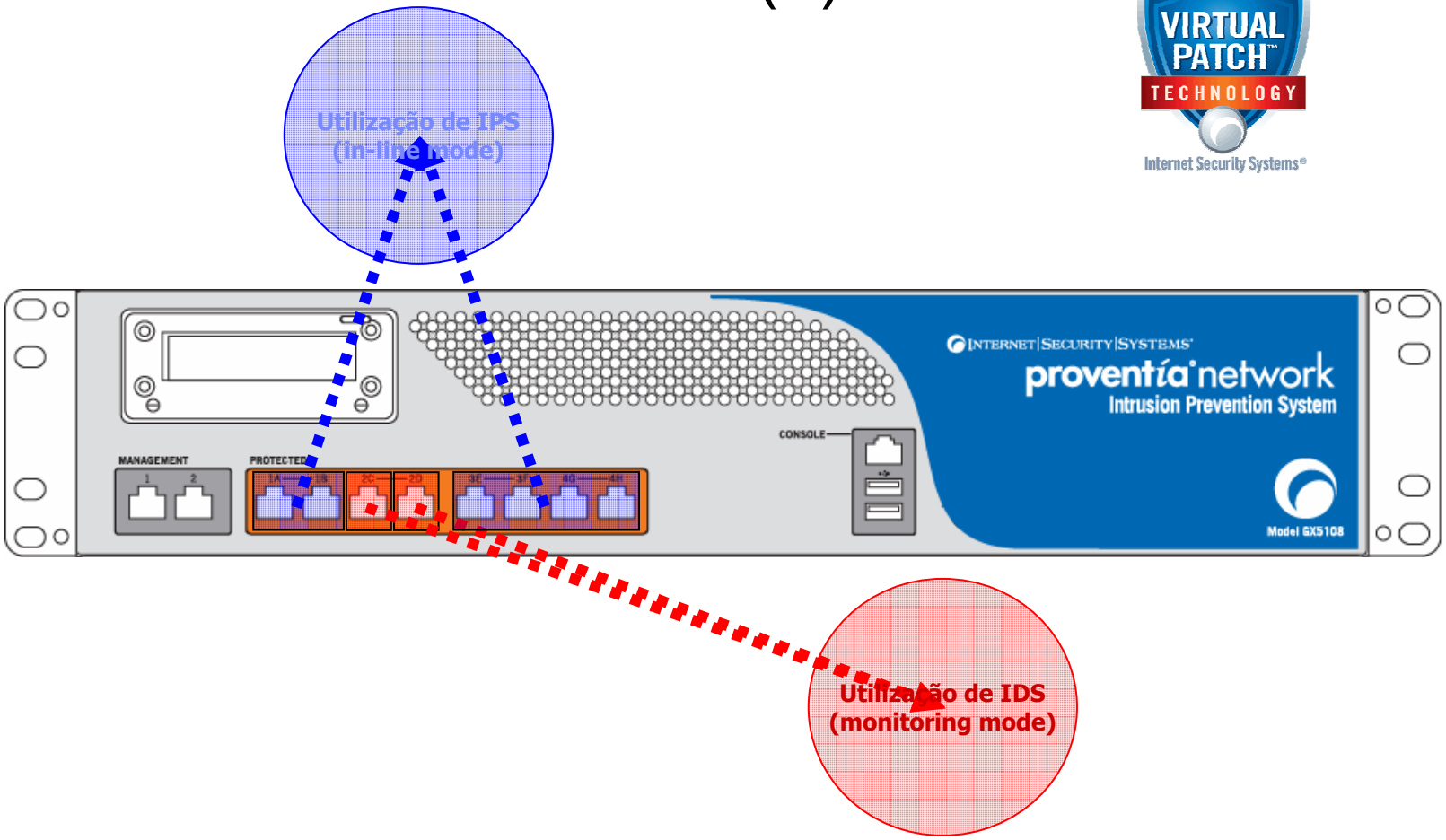
IBM Proventía® Network IPS (1)

- Impede que sistemas vulneráveis sejam invadidos.

- Proteção:
  - –*VoIP*;
  - –*SCADA*;
  - –*GTP*;
  - –*Backbones*;
  - –Servidores;
  - –Perímetros;
  - –Etc.



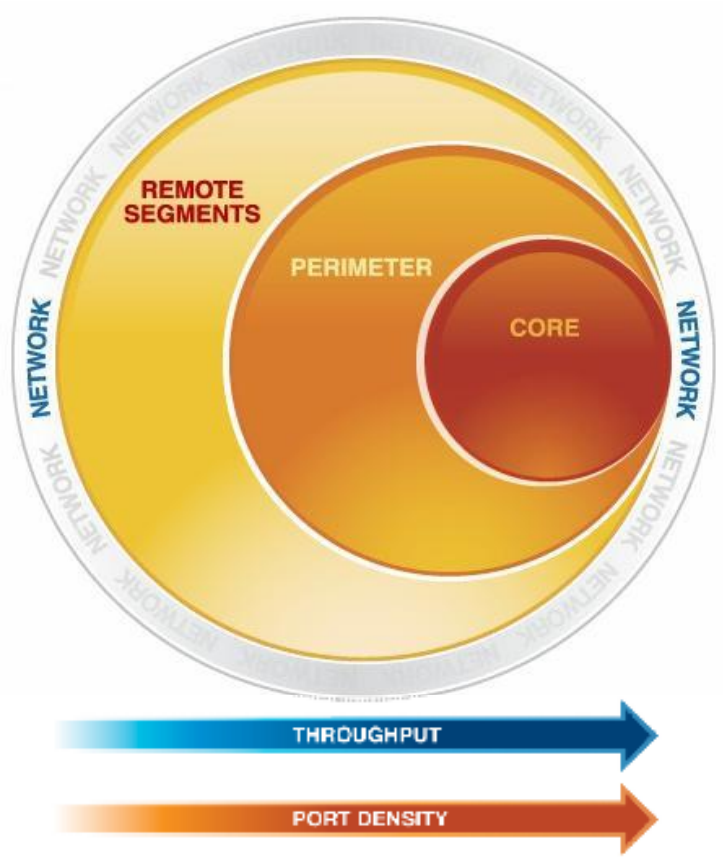
IBM Proventía® Network IPS (2)



IBM Proventía® 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

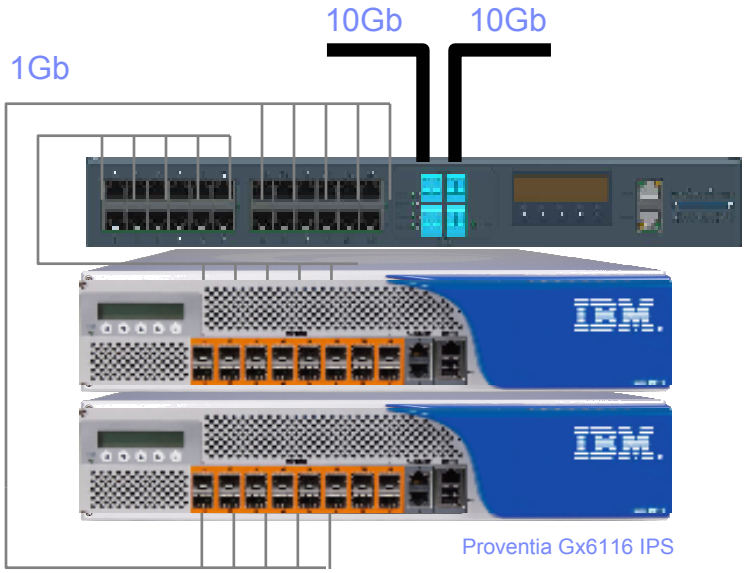
Soluções para um ambiente seguro

IBM Proventia® Network Security Controller

IBM Proventia® Network Security Controller (1)

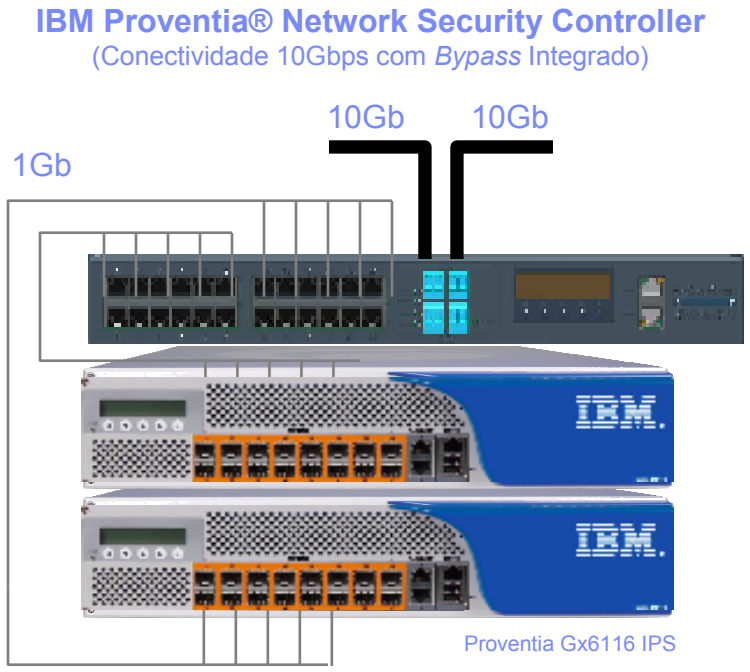
- Proteção para Redes 10 Gbps:
  - Proteção baseada em vulnerabilidades (*World Class*);
  - Fornece conexão 10 Gbps para equipamentos com interfaces 1 Gbps (GX6116 & GX5208);
  - Combina o poder de múltiplos equipamentos para proteção 10 Gbps integral.
- Estende a vida útil de um investimento prévio:
  - 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)

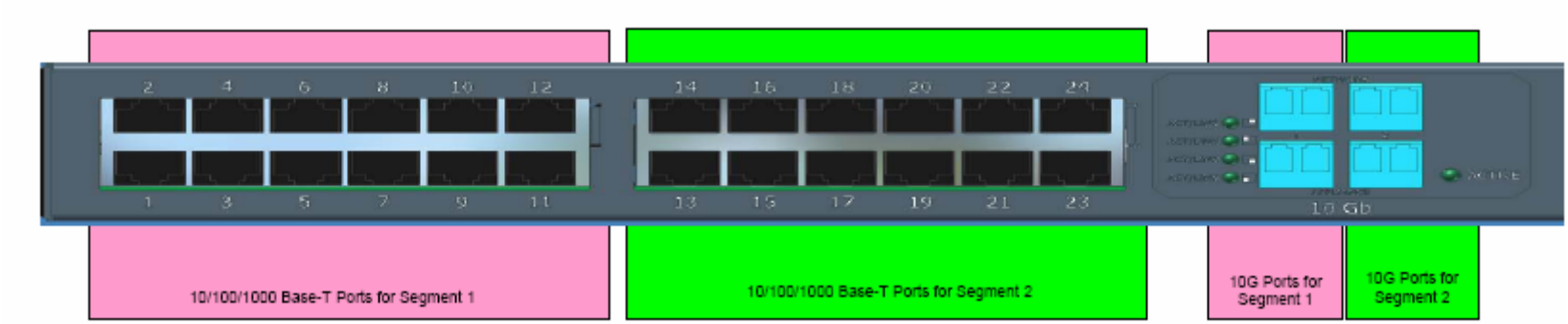


IBM Proventia® Network Security Controller (2)

- 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.*

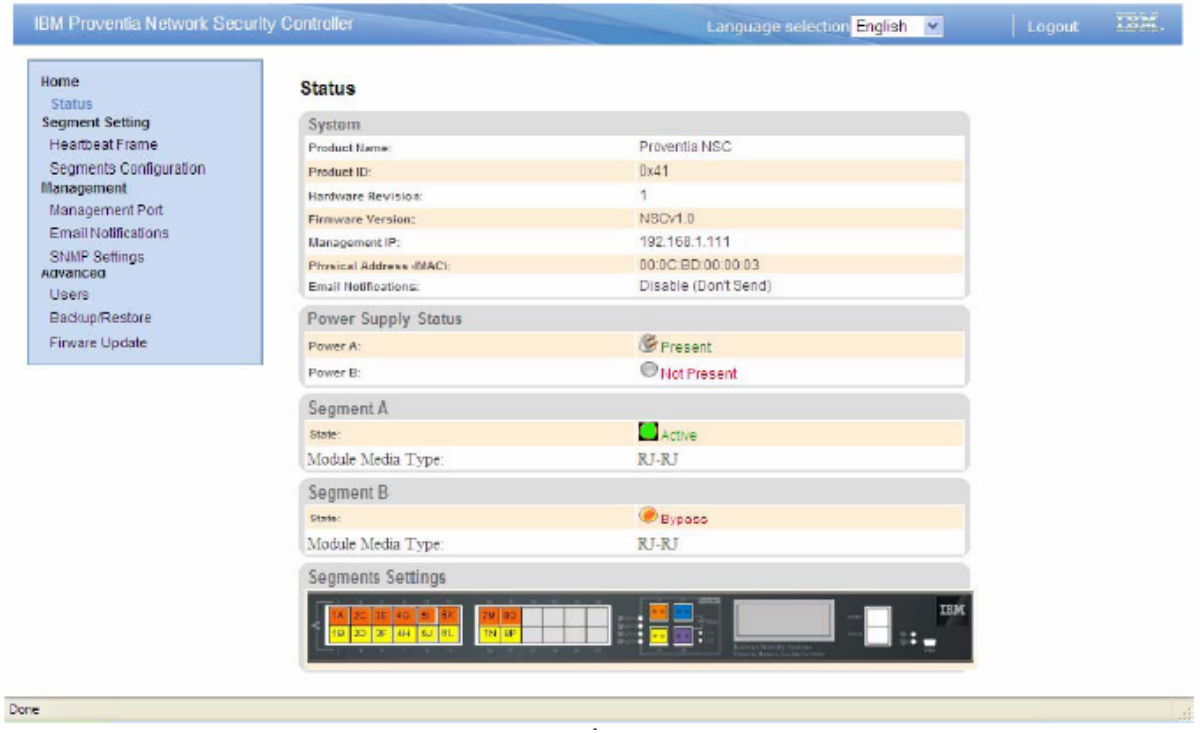


IBM Proventia® Network Security Controller (3)



IBM Proventia® Network Security Controller (4)

Status Page



IBM Security Forum

Soluções para um ambiente seguro

IBM Proventia® Network IPS for Crossbeam®

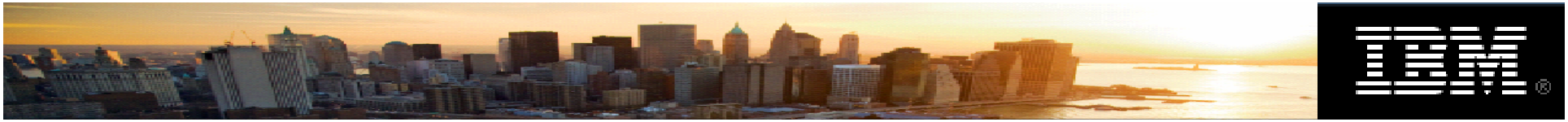
IBM Proventia® IPS for Crossbeam® (1)

- 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 Proventía® Network IPS;
  - Desenvolvido para alto-desempenho, alta-disponibilidade e escalabilidade.

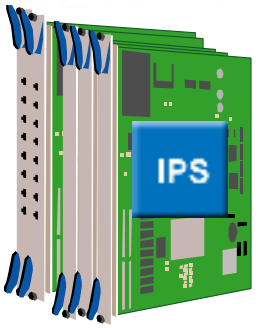
- IBM Internet Security Systems:
  - A mesma proteção preemptiva / preventiva líder de mercado no *Backend*;
  - Proteção baseada em vulnerabilidades (*World Class*).

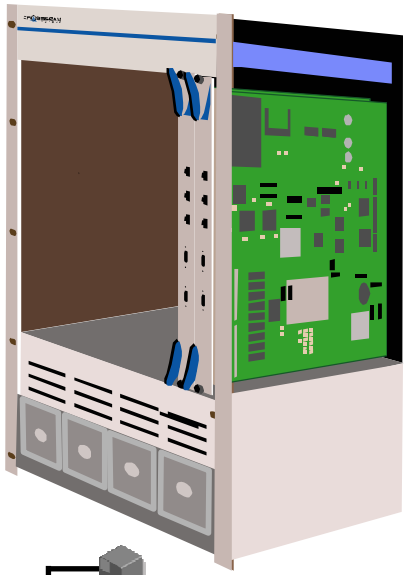
IBM Proventia® IPS for Crossbeam® (2)

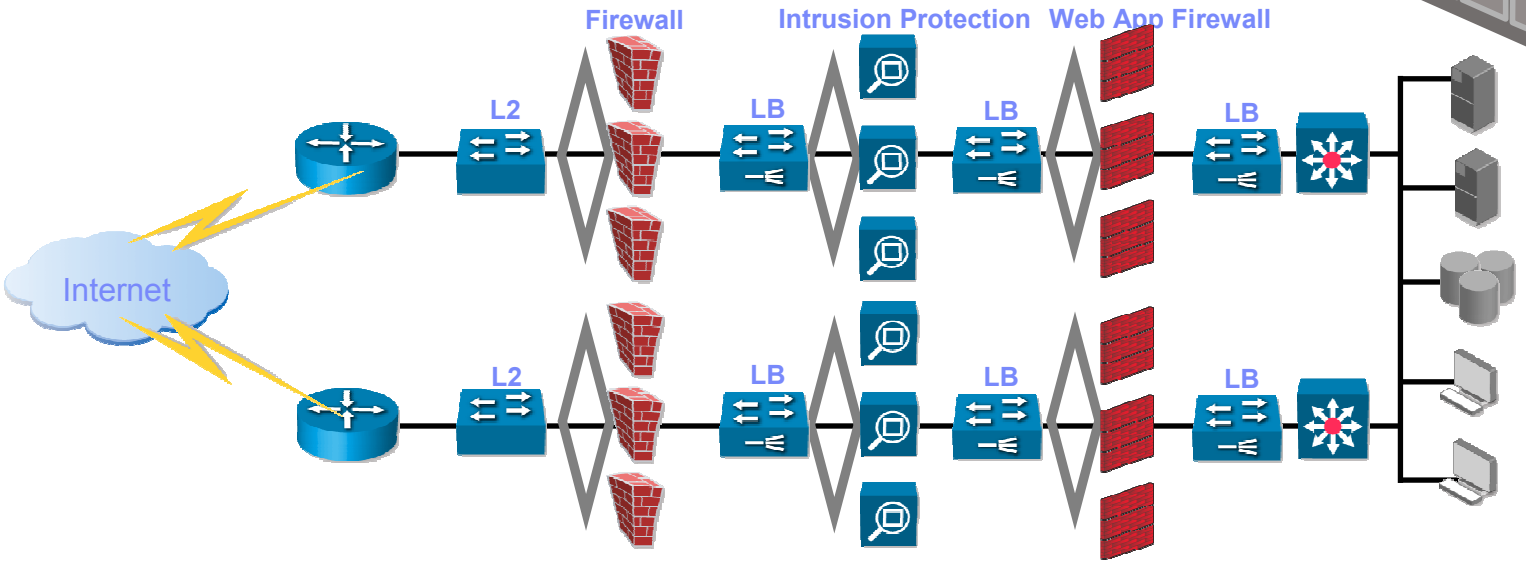
- Virtualização direcionada para:
  - Consolidação;
  - Desempenho.
- Network Processor Modules:
  - Políticas de *Switch* e *Load-Balance*.
- Application Processor Modules:
  - Aplicações de segurança virtuzalidadas.
- Control Processing Modules:
  - Monitoração de *High-Availability*, *Fail-Over*,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



CROSSBEAM SYSTEMS



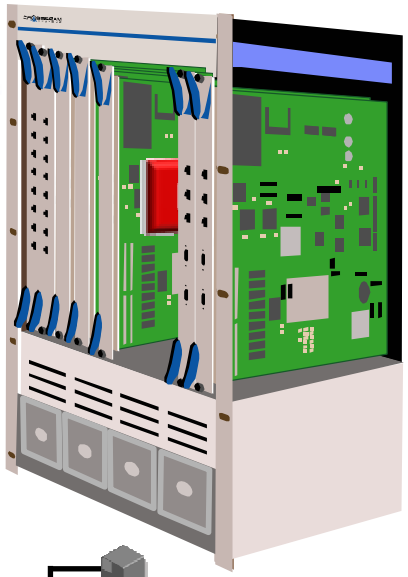


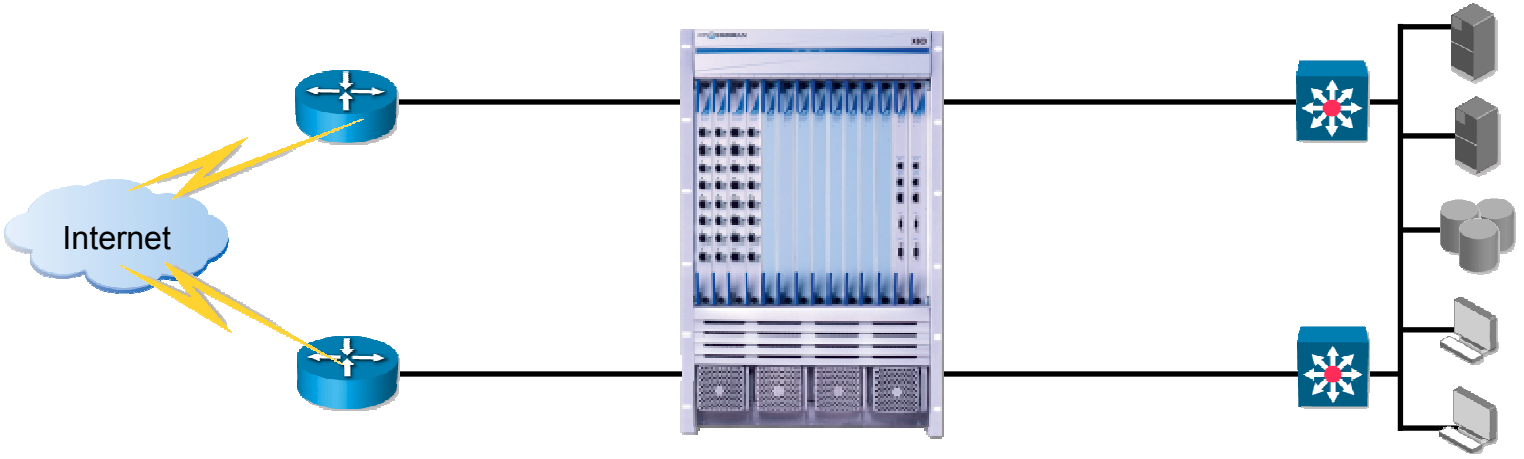


IBM Security Forum

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

Obrigado!

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

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