UTM - POLICIES

Todos os recursos de gerenciamento dos serviços UTM, *"*Filtro de conteúdo *Web", "*Filtro e controle de aplicativos da *WEB 2", "*Interceptação *SSL", "Deep Inspection", "*Roteamento*", "*Controle *QoS (Traffic Shaping)", "*Garantia e prioridade de tráfego*",* "Controle de Cota de tráfego e tempo*", "*Controle de tamanho de arquivos*", "*Filtros de cabeçalho e conteúdo*", "*Balanceamento de *link", "*Múltiplos serviços*", "NAT" e "Proxy",* são aplicados através das políticas.

A definição das regras e políticas de segurança integram em uma mesma interface interativa todos esses recursos, e é possível aplicar em uma mesma política um conjunto de filtros que componham os recursos integrados. A interface permite rastrear todas as políticas a partir de *TAGs* que possibilitam agrupar as regras por finalidade o que facilita os filtros às pesquisas das políticas. As *tags* são adicionadas automaticamente pelo sistema ou o administrador pode definir uma.

1. Em apenas uma interface de configuração, a integração dos recursos em uma política:

- Categoria *WEB*;
- Controle de Aplicativos;
- Controle de Banda;
- Múltiplos Serviços;
- *QoS*;
- Cota de Tempo e Tráfego;
- Escolha de perfil de *link*;
- Escolha de perfil de inspeção profunda;
- Controle de vírus e *Malware*.

2. A configuração ou habilitação dos serviços e recursos, não implicam em criação de uma política de segurança;

3. As políticas de segurança não são aplicadas individualmente em cada serviço.

À Exceção dos serviços *"SD-WAN" e "Firewall",* que contemplam regras ou políticas exclusivas no próprio módulo. Estas não se aplicam as políticas de segurança e sim exclusivamente ao serviço;

4. As políticas de segurança integram [N] condições de análises, que interagem com os diversos recursos de cada serviço, e isso tudo em uma mesma política de segurança.

O que torna o gerenciamento das políticas muito mais fácil e dinâmico para o administrador;

5. As políticas atuam em camadas e o seu comportamento de análise atua no modo "*First Match Wins*". (Literalmente quer dizer... O 1º entre os concorrentes VENCE);

6. As políticas de segurança são cadastradas em grupos e por prioridade e suportam reordenação.

Através da avaliação de *logs* e relatórios estatísticos, é possível reavaliar as prioridades e reordenar as políticas de segurança, de acordo o volume ou importância do tráfego.
Por consequência melhora no desempenho do servidor;

7. As ações das políticas de segurança são:

- Permitir;
- Negar;
- Rejeitar.

Estes são os primeiros conceitos básicos que você deve conhecer.

Recursos das políticas de *compliance*

- **Método de operação:**
  - *First-match wins*;
  - Ordenação por prioridade.

Relação direta com o desempenho do *firewall* suporta a funcionalidade *multithread* que disponibiliza o máximo proveito dos processadores. Permite ordenar as regras, de modo que as políticas ou regras mais utilizadas sejam colocadas acima das políticas menos utilizadas, resultando em mais velocidade para as análises.

A definição das regras e políticas atendem as seguintes especificações e conjunto de filtros e condições para as tomadas de ação.

Abaixo lista das *"Ações"* ***VERSUS*** *"Condições das regras"*:

Tabela 1 - Ações de uma Política

Ações	
Allow	Permitir
Deny	Negar
Reject	Rejeitar

VERSUS...

Tabela 2 - Condições das Regras

Condição POR:	**Condições das políticas:**
Servidor	Uma mesma regra pode ser aplicada para múltiplos servidores; Configurada em uma mesma tela.
Properties	*Name*; *Description*; *Tags*; *Action*; *Policy Group*; *Position*; *Enable traffic logging*; *Time*/*Period*/*Date*.
Connection	***Source*** *Network Zone*; *Network Interface*; *IP Address*; *MAC Address*; ***Destination*** *IP Address*; *Service*. ***Identification*** ***Authenticated*** (*Users*/ *Groups*);

Content	***Web Proxy*** *FTP*; *HTTP*; *HTTPS*; *SSL Inspection*; *Validate SSL certificate*; *SSL Common Name*; *Malware Scanning*; *Explicit Proxy*. ***Web Filter*** *Web Categories*; *Applications*; *URL Filter*; *Browsers*; *HTTP method*; ***Email Protection*** *SMTP*; *POP3*.
Control	***Surfing Control*** *Content-Type Filter*; *HTTP Filter Header*; *Filter*; ***Surfing Quotas*** *Maximum Time*; *Maximum Traffic*; *Max Download Size*; *Max Upload Size*.
Security	***Deep Inspection*** *Sensor*. ***Threat Blocking*** *Compromised Addresses*; *Geolocation*. ***Packet Filter*** *TTL*; *Package Type*; *Packet Content*; *TCP MSS*.
Routing	***Gateway*** *NAT*; *SD-WAN*. ***QoS*** *Traffic Shaping*; *Flag packets* (*TOS*); *Flag packets* (*DSCP*).

As definições são idênticas para *IPv4* e *IPv6*, sofrendo alterações somente em seus endereçamentos e algumas características proprietária de cada versão do protocolo.

Policies

Contém as opções:

- IPv4;
- IPv6.