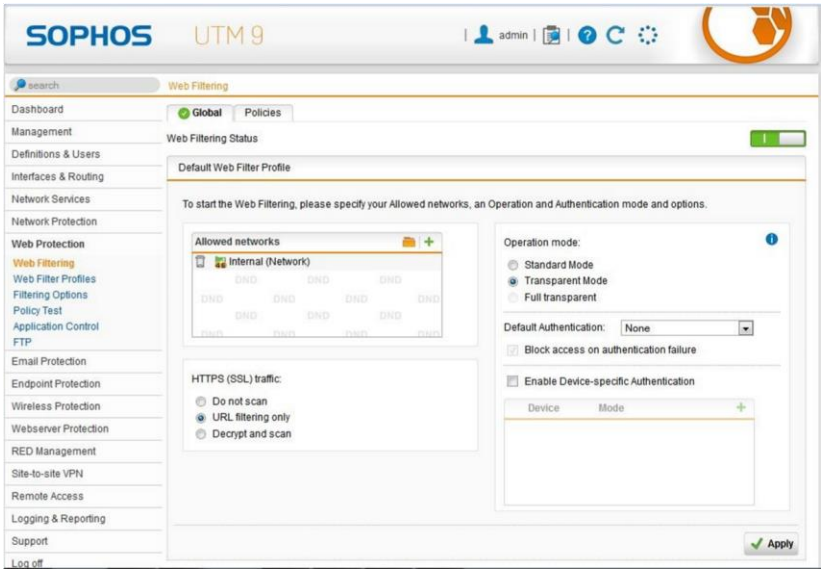
Configurações Básicas para ativar e configurar o WebProtection

- Descrição:

Este manual descreve os procedimentos necessários para realizar uma configuração básica do Web Protection.

- O que fazer?

1. Acesse o **WebAdmin;**
2. Clique em **WebProtecion;**
3. Ative a chave conforme imagem abaixo;



4. Nesta tela é informado as configurações gerais do equipamento, ou seja, o que será configurado para todos das redes configuradas.
5. Em "**Allowed networks**" especifique as redes que usarão o serviço de **proxy**.
6. Abaixo da opção anterior haverá a opção "**HTTPS (SSL) traffic:**",
   - Selecione se você deseja que os pacotes de navegação sejam, **descriptografados** e analisados.
   - Se será analisado somente a **URL** do conteúdo filtrado.
   - Ou não terá nenhum tipo de escaneamento para conteúdos **SSL**.
7. Em **Operation mode**, marque a opção que o equipamento trabalhará com os hosts, ou seja, se o modo de operação será Explicito nos navegadores ou trabalhará de forma Transparente.
8. **Default Authentication**, selecione se todos que consultarem o proxy deverão ou não autenticar-se durante o processo de acesso a internet, existem as seguintes opções:

8.1 - Opções de autenticação do Proxy **Transparente**;

- **Active Directory SSO**, opção que permite a autenticação direta com os usuários do AD já vinculados com o UTM.
- **Agent**, opção que permite você a usar o **client** da Sophos instalado na maquina host para autenticação do usuário no proxy.
- **Browser**, permite a autenticação dos usuários via navegador.
- **None**, sem autenticação.

8.2 - Opções de autenticação do Proxy **Standart/Explicito**;

- **Active Directory SSO**, mesma opção citada no proxy **transparente**.
- **Agent**, mesma opção citada no proxy **transparente**.
- **Apple OpenDirectory SSO**, permite a autenticação para os usuários que usam este tipo de sistema.
- **Basic User Authentication**, abre um pop-up para o usuário autenticar quando iniciado o navegador.
- **Browser**, mesma opção citada no proxy **transparente**.
- **eDirectory SSO**, permite a autenticação para os usuários que usam este tipo de sistema.

8.3 - **Block access on authentication failure**, marque esta opção caso você queira bloquear os usuários que não conseguiram autenticar-se em uma das opções selecionadas de autenticação.

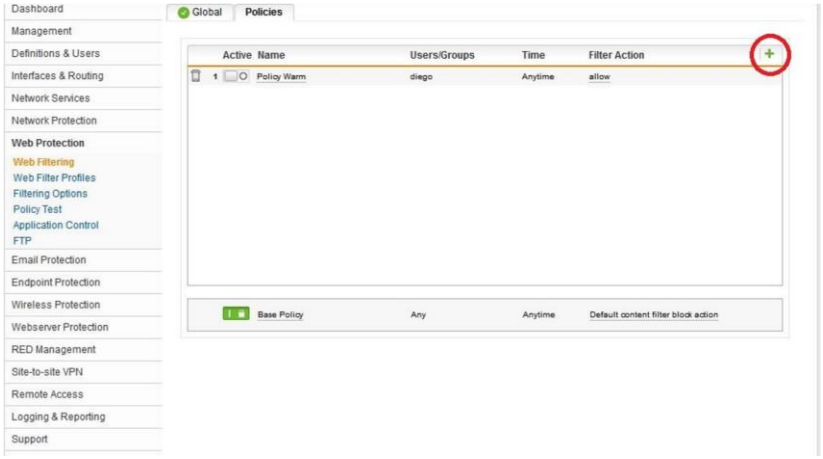
8.4 - **Enable Device-specific Authentication**, caso você queira criar uma autenticação diferenciada para algum tipo de dispositivo, marque esta opção e especifique quem terá a autenticação diferenciada de acordo com as seguintes opções:

- **Windows;**
- **Mac OS;**
- **Linux;**

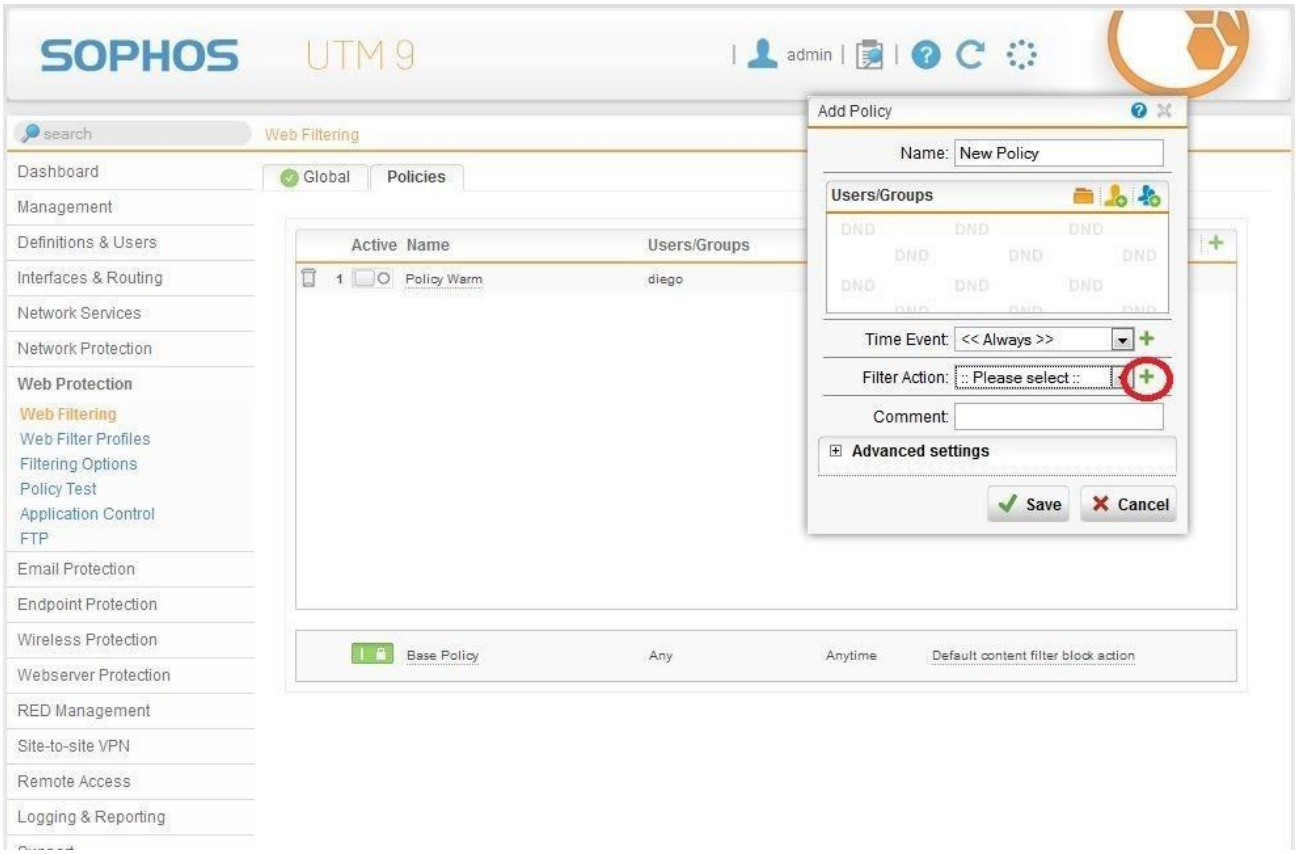
- **iOS;**
- **Android;**
- **Kindle;**
- **Blackberry;**

- Clique em **Apply** e passe para a aba "**Policy**";

9. Na aba Policy clique no ícone que representa o "+";



9.1 - Abrirá a seguinte tela;



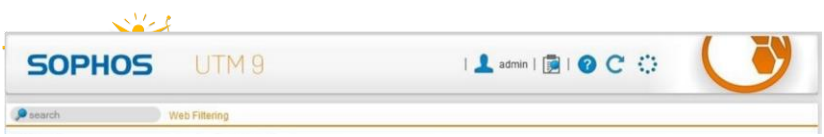
9.2 - Defina um nome para a Politica;

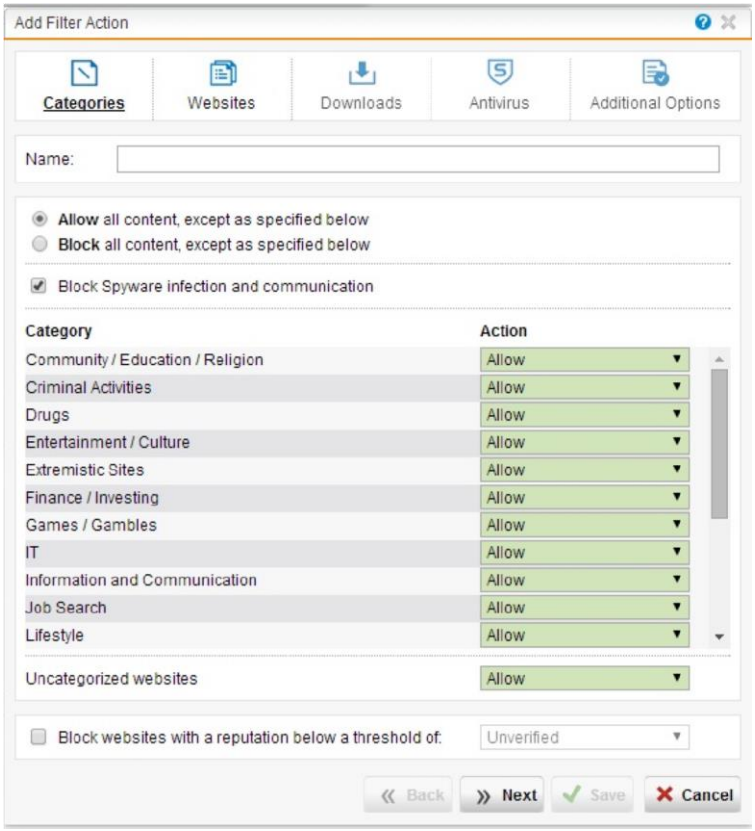
9.3 - Em "**User/Groups**" cadastre todos os usuários que entrarão nas regras que serão criadas, caso a regra seja para todos usuários da rede, não será necessário especificar nada neste campo.

9.4 - **Time Event**, caso esta regra seja aplicada apenas em um determinado horário, você poderá especificar aqui esta configuração, caso contrario, se a regra for aplicada em qualquer horário, deixe conforme a imagem especifica.

9.5 - **Filter Action**, clique no ícone "+" para iniciar a configuração de uma nova regra de filtro que será aplicado para este grupo.

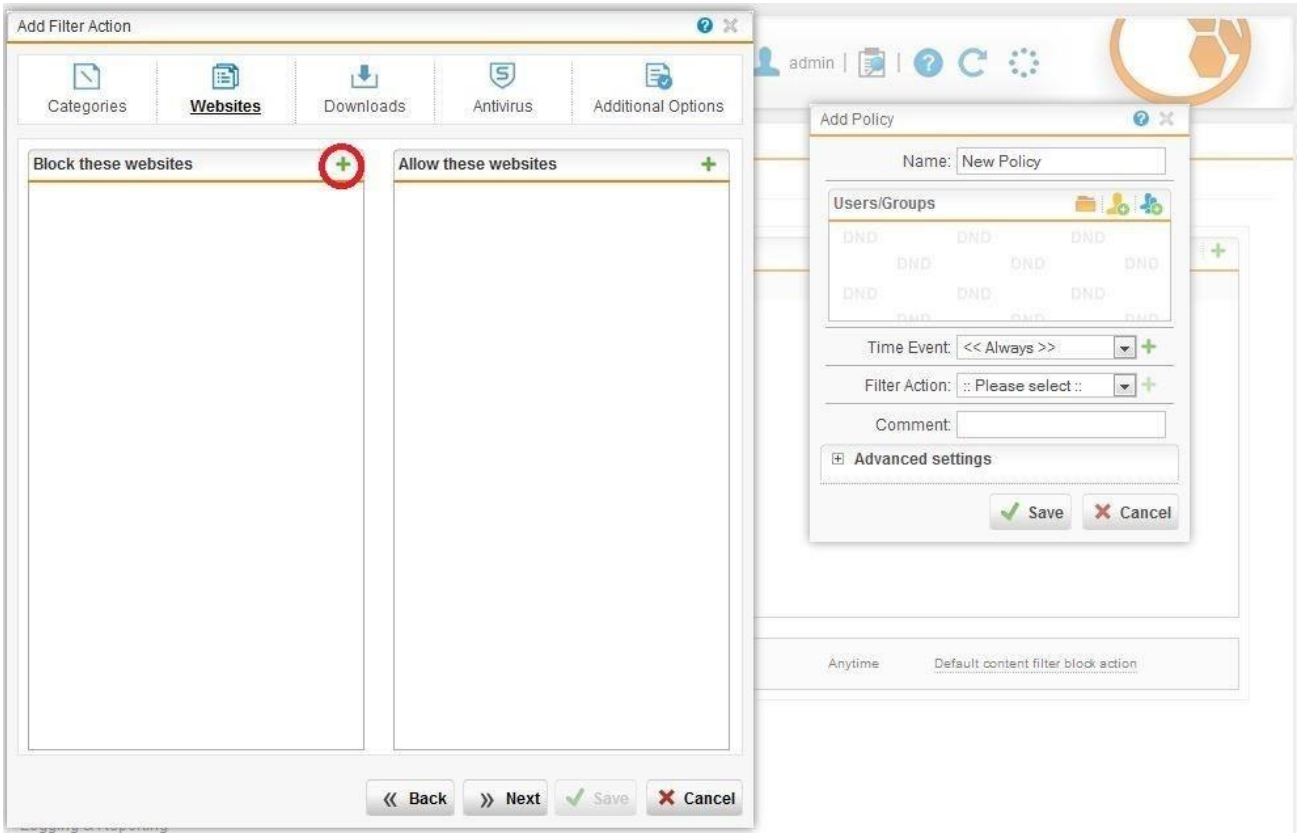
9.6 - Clicando no ícone abrirá a seguinte tela;



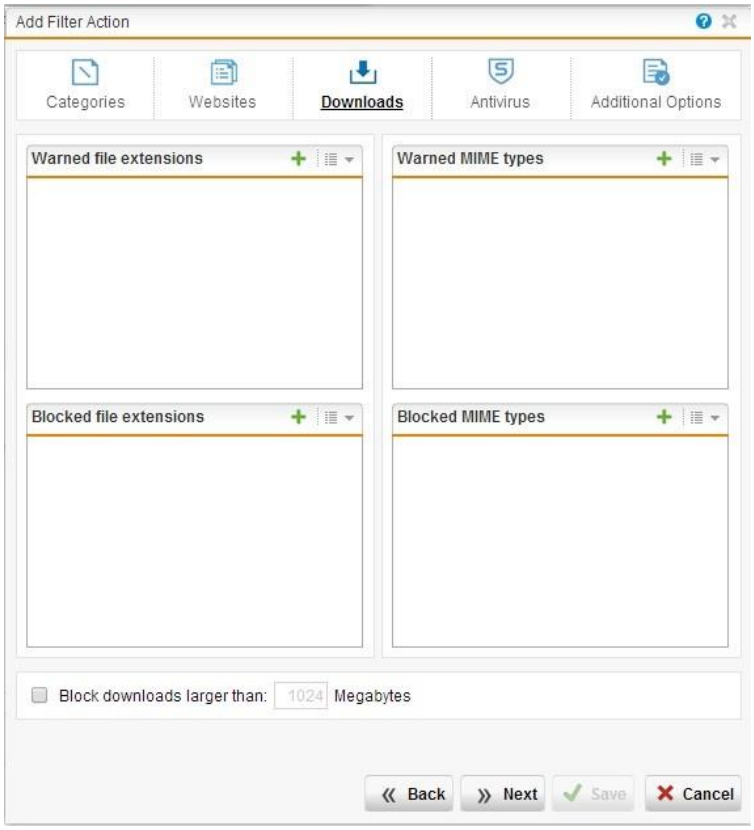


9.7 - Existem uma série de categorias já definidas pela Sophos para nos ajudar a iniciar os filtros desejados em nossa rede, a aba **"Categories"** irá permitir que você **libere** uma categoria, **Alerte** o acesso na mesma ou realize o **bloqueio**.

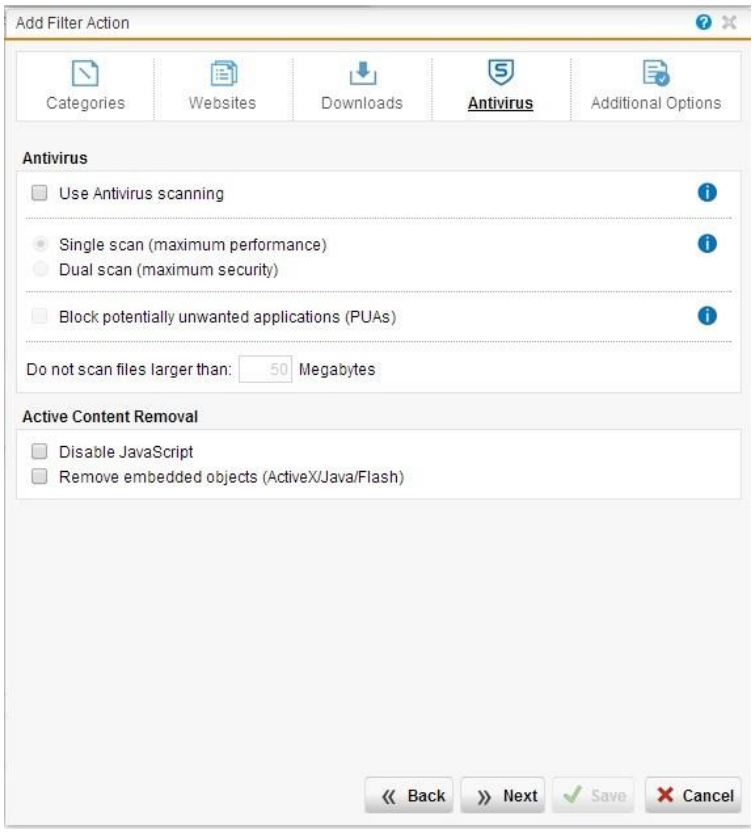
9.8 - Na aba **Websites**, configure os sites que sempre serão bloqueados e/ou liberados independente das categorias .



9.9.1 - Na aba "**Downloads**" você terá as opções de **bloquear** extensões e MIME types para download bem como **alertar** o uso das mesmas.

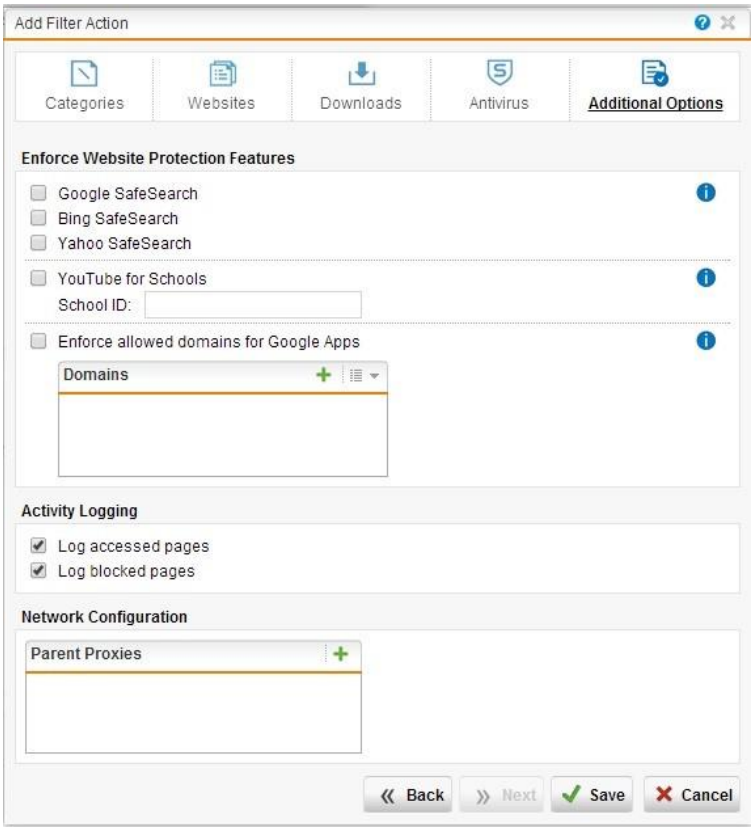


9.9.2 - Aba **Antivirus** determine se as paginas passarão ou não por uma ou duas engines de verificação e se os PUAS deverão ser bloqueados ou não durante o processo de verificação.



9.9.3 - Por ultimo a aba **Additional Option**, você poderá forçar com que os usuários usem o Safe Search dos buscadores como o Google, Yahoo e Bing.

- Utilizar o **Youtube for Schools**, você poderá restringir o acesso Youtube, porém liberar uma determinada pagina do mesmo para acesso dos usuários entre outras funções.



10. Salve as configurações.
11. Agora você acabou de criar as primeiras regras de proxy e poderá usar este modelo para criar as demais regras para sua rede principal.

- Pré-requisitos de implantação do proxy

Para implantar o Web Protection do Sophos UTM existem alguns requisitos que devem ser seguidos para um bom funcionamento dos filtros na rede, segue abaixo relação entre os tipos de implantação e seus requisitos: - **Modo Transparente**

Ao utilizar o modo transparente como modo de implantação do proxy para sua rede, você deverá avaliar dois requisitos.

1° - Este requisito exige que todas as máquinas tenham o Sophos UTM como gateway da rede, ou o gateway do seu ambiente deverá fazer o roteamento dos pacotes destinados á internet para o UTM, para que o mesmo consiga realizar o tratamento dos pacotes.

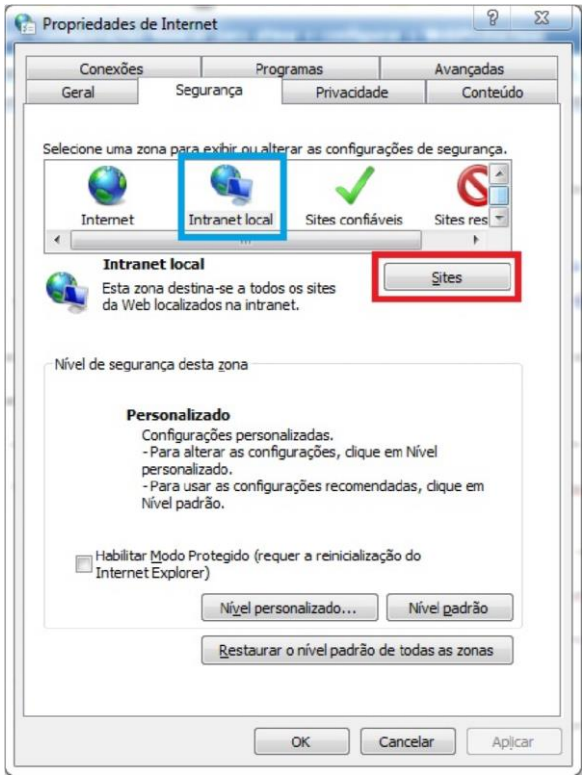
2° - Caso você opte pelo **SSO** com o **Active Directory** no modo transparente, você deverá realizar as seguintes ações:

- Configurar o DNS das máquinas de toda rede interna para que resolvam o hostname do UTM vinculado ao IP interno do UTM.

- Configurar em todas as máquinas que usarão este tipo de autenticação os seguintes passos:

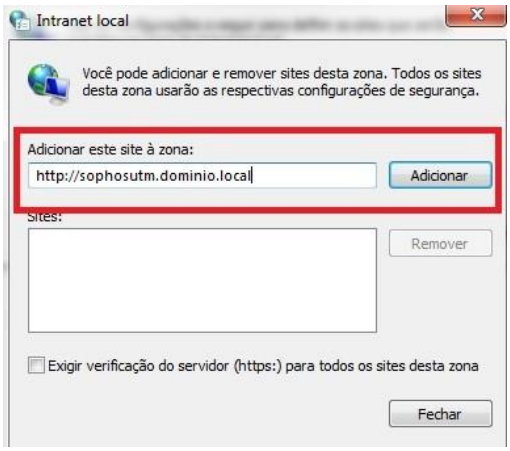
- Acesse as configurações de segurança do navegador.

- Selecione a opção "**Intranet local**" e depois clique em "**Sites**" conforme a imagem abaixo:



- Clique em Avançadas:

- Adicione o Hostname do UTM conforme a imagem abaixo sugere:



- Verifique se o **SSO** está funcionando.

- **Modo Explicito**

Para ativar o modo explicito nas máquinas existe apenas um requisito e este é especificar quem é o servidor de proxy na rede nos navegadores das máquinas.